
# NAVAL POSTGRADUATE SCHOOL

**MONTEREY, CALIFORNIA**

# THESIS

**TEXAS SHOULD REQUIRE HOMELAND SECURITY STANDARDS FOR HIGH-SPEED RAIL**

by

Steven M. Polunsky

December 2015

Thesis Advisor: Thomas Mackin
Second Reader: Allan Rutter

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

| REPORT DOCUMENTATION PAGE | | | Form Approved OMB No. 0704–0188 |
|---|---|---|---|
| Public reporting burden for this collection of information is estimated to average 1 hour per response including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503. | | | |
| **1. AGENCY USE ONLY** *(Leave blank)* | **2. REPORT DATE** December 2015 | **3. REPORT TYPE AND DATES COVERED** Master's thesis | |
| **4. TITLE AND SUBTITLE** TEXAS SHOULD REQUIRE HOMELAND SECURITY STANDARDS FOR HIGH-SPEED RAIL | | **5. FUNDING NUMBERS** | |
| **6. AUTHOR(S)** Steven M. Polunsky | | | |
| **7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)** Naval Postgraduate School Monterey, CA 93943-5000 | | **8. PERFORMING ORGANIZATION REPORT NUMBER** | |
| **9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)** N/A | | **10. SPONSORING / MONITORING AGENCY REPORT NUMER** | |
| **11. SUPPLEMENTARY NOTES** The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB protocol number ____N/A____. | | | |
| **12a. DISTRIBUTION / AVAILABILITY STATEMENT** Approved for public release; distribution is unlimited | | **12b. DISTRIBUTION CODE** A | |

**13. ABSTRACT (maximum 200 words)**

A private corporation is proposing a high-speed intercity passenger train system to operate between Dallas and Houston using Japanese technology and methods. This project brings with it an array of unique and unprecedented homeland security issues. Train bombings in Madrid and London and attacks on high-speed trains elsewhere raise questions about the security of such transportation. A modern high-speed rail system is a network of potential vulnerabilities, and terrorist groups have identified public transportation as desirable targets. Should the State of Texas require homeland security standards for high-speed rail?

A review of the literature reveals the number and consequences of terrorist actions against passenger rail in general and intercity high-speed trains in particular. In addition, it suggests that this writing is the first in its specific application. This thesis places the project in historical and geographical context and reviews potential vulnerabilities using a framework developed by the Argonne National Laboratory. Furthermore, it includes a fault tree analysis and an options analysis through which possible approaches are identified and analyzed. Finally, this thesis finds that the State of Texas should require homeland security standards and provides recommendations for action in the areas of law enforcement, cybersecurity, intelligence, privacy, screening, psychological and mental health effects, and community involvement.

| **14. SUBJECT TERMS** homeland security, high-speed rail, passenger trains, transit, Texas, transportation, terrorism, railroad, trains, intel, intelligence, cyber, energy, Japan, Texas A&M Transportation Institute | | | **15. NUMBER OF PAGES** 113 |
|---|---|---|---|
| | | | **16. PRICE CODE** |
| **17. SECURITY CLASSIFICATION OF REPORT** Unclassified | **18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified | **19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified | **20. LIMITATION OF ABSTRACT** UU |

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

# TEXAS SHOULD REQUIRE HOMELAND SECURITY STANDARDS FOR HIGH-SPEED RAIL

Steven M. Polunsky
Research Scientist, Texas A&M Transportation Institute
B.A., The University of Texas at Austin, 1981
M.P.A., The University of Texas, 1983

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES**
**(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL**
**December 2015**

Approved by: Thomas Mackin
Thesis Advisor

Allan Rutter, Texas A&M Transportation Institute
Second Reader

Erik Dahl
Associate Chair of Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

# ABSTRACT

A private corporation is proposing a high-speed intercity passenger train system to operate between Dallas and Houston using Japanese technology and methods. This project brings with it an array of unique and unprecedented homeland security issues. Train bombings in Madrid and London and attacks on high-speed trains elsewhere raise questions about the security of such transportation. A modern high-speed rail system is a network of potential vulnerabilities, and terrorist groups have identified public transportation as desirable targets. Should the State of Texas require homeland security standards for high-speed rail?

A review of the literature reveals the number and consequences of terrorist actions against passenger rail in general and intercity high-speed trains in particular. In addition, it suggests that this writing is the first in its specific application. This thesis places the project in historical and geographical context and reviews potential vulnerabilities using a framework developed by the Argonne National Laboratory. Furthermore, it includes a fault tree analysis and an options analysis through which possible approaches are identified and analyzed. Finally, this thesis finds that the State of Texas should require homeland security standards and provides recommendations for action in the areas of law enforcement, cybersecurity, intelligence, privacy, screening, psychological and mental health effects, and community involvement.

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

# LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| ANL | Argonne National Laboratory |
| CEO | chief executive officer |
| CIA | Central Intelligence Agency |
| CRS | Congressional Research Service |
| DHS | Department of Homeland Security |
| DPS | [Texas] Department of Public Safety |
| EIS | Environmental Impact Statement |
| EPA | Environmental Protection Agency |
| FBI | Federal Bureau of Investigation |
| FRA | Federal Railroad Administration |
| GAO | Government Accountability Office |
| HSR | high-speed rail |
| Intel | intelligence |
| IT | information technology |
| JCIC | Joint Crime Information Center |
| JRC | Central Japan Railway Company |
| N700-I | model/version of Shinkansen high-speed train |
| NEPA | National Environmental Policy Act |
| NPA | National Police Agency of Japan |
| NTSB | National Transportation Safety Board |
| O&M | operating and maintenance |
| RSC | rail security coordinator |
| SCADA | supervisory control and data acquisition |
| TCIPC | Texas Critical Infrastructure Protection Council |
| TCR | Texas Central Railway/Texas Central High-Speed Railway |
| TGV | train à grande vitesse—France's high-speed train |
| TMFD | Tokyo Metropolitan Fire Department |
| TMPD | Tokyo Metropolitan Police Department |
| TPWD | Texas Parks and Wildlife Department |
| TSA | Transportation Security Administration |

| | |
|---|---|
| TxDOT | Texas Department of Transportation |
| USAF | U.S. Air Force |
| U.S. DOT | U.S. Department of Transportation |

# EXECUTIVE SUMMARY

From 2004 to 2008, terrorists killed over 2000 people and injured over 9000 more in 530 separate attacks targeting passenger rail systems.[1] The Transportation Safety Administration (TSA) considers passenger railroads to be

> high consequence targets in terms of potential loss of life and economic disruption as they carry large numbers of people in a confined environment, offer the opportunity for specific populations to be targeted at particular destinations, and often have iconic structures.[2]

Regarding the more limited subset of high-speed passenger trains (HSR) worldwide, between 1970 and 2012, there were 33 high-speed rail attacks, which killed 32 people.[3] The August 2015 attempted French high-speed train terrorist attack is a reminder that intercity high-speed passenger trains are likely targets for terrorism.

While cyberattacks have occurred,[4] terrorist attacks on passenger rail systems have primarily targeted physical systems, notably Madrid in 2004, London in 2005, Mumbai in 2006, and Kunming in 2014. The French HSR line is fenced, but in 1995, saboteurs penetrated the fence and planted a bomb. Tragedy was averted when the bomb failed to explode.[5]

The Texas Central Railway (TCR), a private corporation, is proposing a high-speed intercity passenger train system to operate between Dallas and Houston[6] using

---

[1] Nabajyoti Barkakati, and David Maurer, *Technology Assessment: Explosives Detection Technologies to Protect Passenger Rail* (Washington, DC: U.S. Government Accountability Office, 2010), 12.

[2] 73 Fed. Reg. 72130 (2008).

[3] Brian Michael Jenkins et al., *Formulating a Strategy for Securing High-Speed Rail in the United States* (San Jose, CA: Mineta Transportation Institute, 2013), 9.

[4] Aliya Sternstein, "Hackers Manipulated Railway Computers, TSA Memo Says," NextGov, January 23, 2012, http://www.nextgov.com/cybersecurity/2012/01/hackers-manipulated-railway-computers-tsa-memo-says/50498/.

5 Brian Michael Jenkins, Bruce R. Butterworth, and Jean-Francois Clair, *The 1995 Attempted Derailing of the French TGV (High-Speed Train) and a Quantitative Analysis of 181 Rail Sabotage Attempts* (San Jose, CA: Mineta Transportation Institute, 2010).

[6] Jody Serrano, "High-Speed Rail Firm's Chief: Public Meetings Set for Proposal," *The Texas Tribune,* September 20, 2014.

Japanese technology and methods.[7] TCR proposes a 205-mph train;[8] however, existing high-speed rail in the U.S. does not exceed 110 mph, except for a 28 mile stretch of 150 mph-capable track in the northeast.[9] This is not the first high-speed rail proposal for Texas,[10] and there are other proposals in various stages in other states. However, this project has the potential to be the first of its kind implemented in the country, which one writer has said would "be a transformative event in the history of the nation's transportation system."[11]

Through the Transportation Security Administration (TSA), the federal government has security oversight for passenger rail systems. Its approach for rail is similar to that for intercity buses, as opposed to the screening and security levels provided for air transportation. State homeland security requirements and programs for Texas are authorized by Chapter 421 of the Texas Government Code.[12] The statutes require the governor to develop a homeland security strategy with specific plans for protecting critical infrastructure and coordinating with other public and private sector entities, among other duties.

Current statutory guidance and requirements regarding critical infrastructure protection are minimal and broad. If a first-of-its-kind, large-scale, privatized infrastructure project, which presents an attractive target for terrorists, goes into revenue service, the paradigm will have shifted. The security framework may well be tested under real-world conditions with any shortcomings becoming glaringly apparent.

---

[7] Ibid.

[8] Aman Batheja, and Stephen J. Smith, "The Bullet Train that Could Change Everything," *The Texas Tribune*, August 18, 2014.

[9] Yonah Freemark, "Why Can't the United States Build a High-Speed Rail System?" The Atlantic's CityLab, August 13, 2014, http://www.citylab.com/politics/2014/08/why-cant-the-united-states-build-a-high-speed-rail-system/375980/.

[10] Marc H. Burns, *High-Speed Rail in the Rear-View Mirror: A Final Report of the Texas High-Speed Rail Authority* (Austin, TX: MH Burns, 1995).

[11] Batheja, and Smith, "The Bullet Train that Could Change Everything."

[12] Texas Legislative Council, *Texas Government Code, Chapter 421: Homeland Security* (Austin, TX: Texas Legislative Council, 2003).

Short of statutory change, the state does not appear to have the ability to impose any security standards or requirements on the project, which raises these questions: should the train operators be required to participate in intelligence-gathering efforts? Is it in the state's interest to mandate a level of law enforcement presence, either on board the train or at stations? Will financial backers of the Texas Central Railway (TCR) system require security standards, both as a means of protecting the asset and its ability to generate revenue to repay its debts?

The Argonne National Laboratory[13] has created a framework for use in evaluating site security[14] that lists six major components: security management, physical security, information sharing, security force, dependencies, and protective measures.[15] Evaluating these components through selected subcomponents and applying the utility tree analysis outlined by Morgan D. Jones,[16] along with probability and fault tree analysis, yields a number of possible options and approaches. This results in a finding that the State of Texas should require homeland security standards for HSR. Given the unique and precedent setting nature of the project, the legislature should be proactive in creating specific requirements or expectations. In addition, it should ensure state enforcement agencies have sufficient authority to ensure the provision of public safety for a private sector transportation project. These requirements may include a legal ability to acquire and enforce representations made regarding the system's security provisions and also should address how law enforcement is achieved, how the project interacts with the intelligence community, and baseline requirements for cyber security, passenger data privacy, vulnerability and threat assessment, and community considerations and involvement along the route.

---

13 "Better Infrastructure Risk and Resilience," Argonne National Laboratory, last modified August, 2010, accessed October 6, 2015, http://www.anl.gov/articles/better-infrastructure-risk-and-resilience.

14 U.S. Department of Homeland Security. "Enhanced Critical Infrastructure Protection," last modified September 9, 2015, accessed October 6, 2015, http://www.dhs.gov/ecip.

15 Robert E. Fisher et al., Constructing Vulnerability and Protective Measures Indices for the Enhanced Critical Infrastructure Protection Program (No. ANL/DIS-09-4), (Argonne, IL: Argonne National Laboratory, 2009), http://www.osti.gov/scitech/biblio/966343.

16 Morgan D. Jones, *The Thinker's Toolkit: Fourteen Powerful Techniques for Problem Solving* (New York: Three Rivers Press, 1998), 252.

THIS PAGE INTENTIONALLY LEFT BLANK

# ACKNOWLEDGMENTS

I would like to acknowledge the faculty and staff of the Naval Postgraduate School's Center for Homeland Defense and Security, along with the students of Cohort 1403/1404, for generously sharing their guidance, assistance, and ideas over the course of my degree program. Much appreciation goes to Dr. Carolyn Halladay, Dr. Lauren Wollman, Dr. Tom Mackin, and Allan Rutter, all of whom played crucial roles in the development of this thesis. Participating in this program could not have been attempted, much less completed, without the early encouragement of John Carona and Margie McCloskey; the good advice of Angi English; the support of many people at the Texas A&M Transportation Institute, for all of whom I am grateful; and of course, the loving patience of my wife, Lauri.

THIS PAGE INTENTIONALLY LEFT BLANK

# I. OVERVIEW

State homeland security requirements and programs for Texas are authorized by Chapter 421 of the Texas Government Code.[1] The statutes require the governor to develop a homeland security strategy with specific plans for protecting critical infrastructure and coordinating with other public and private sector entities, among other duties. While guidance in some areas is specific and conflicting (for example, the Homeland Security Council is constituted in three different ways), guidance and requirements regarding critical infrastructure protection are minimal and broad.

The state can control its own assets and programs, but statutorily and philosophically it has limited control over the private sector. According to the state planning documents, the legislature created several statewide advisory groups to support implementing the plan, including the Texas Critical Infrastructure Protection Council (TCIPC). The TCIPC has both private and public sector participants.[2] However, beyond this voluntary participative measure, there does not appear to be a way to compel cooperation or participation, or even create enforceable requirements, from the state's homeland security perspective.

This inability does not appear to create any significant issues under current conditions. However, if a first-of-its-kind, large-scale, privatized infrastructure project, which presents an attractive target for terrorists, goes into revenue service, the paradigm will have shifted. The security framework may well be tested under real-world conditions with any shortcomings becoming glaringly apparent.

A private corporation is proposing a high-speed intercity passenger train system to operate between Dallas and Houston, Texas[3] using Japanese technology and methods.[4]

---

[1] Texas Legislative Council, *Texas Government Code, Chapter 421: Homeland Security* (Austin, TX: Texas Legislative Council, 2003).

[2] Rick Perry, *Texas Homeland Security Strategic Plan: 2010–2015* (Austin, TX: Texas Department of Public Safety, 2010).

[3] Jody Serrano, "High-Speed Rail Firm's Chief: Public Meetings Set for Proposal," *The Texas Tribune,* September 20, 2014.

[4] Ibid.

The Texas Central Railway (TCR; officially the Texas Central High-Speed Railway, in partnership with the Central Japan Railway Company, or JRC) is leading this effort.[5] The private (publicly traded) JRC currently operates over 300 high-speed trains each day between Osaka and Tokyo.

TCR proposes a 205-mph train;[6] existing high-speed rail in the U.S. does not exceed 110 mph except for a 28 mile stretch of 150 mph-capable track in the northeast.[7] This is not the first high-speed rail proposal for Texas,[8] and there are other proposals in various stages in other states. However, this project has the potential to be the first of its kind implemented in the country, which one writer has said would "be a transformative event in the history of the nation's transportation system."[9] Figure 1 shows the routes in consideration for the project as of October 2015.

[5] "Texas Central Railway: America's Bullet Train," New Magellan Venture Partners, LLC, accessed November 14, 2015, http://newmagellan.com/page8/page11/index.html.

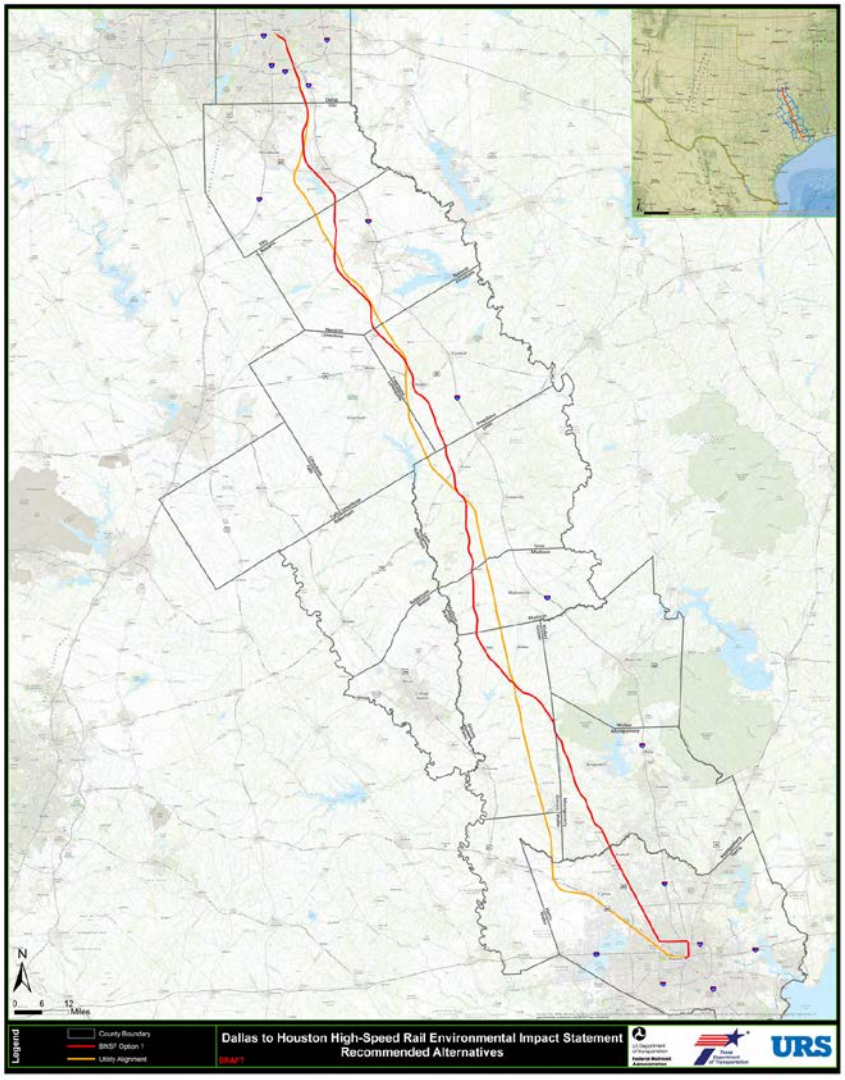
[6] Aman Batheja and Stephen J. Smith, "The Bullet Train that Could Change Everything," *The Texas Tribune*, August 18, 2014.

[7] Yonah Freemark, "Why Can't the United States Build a High-Speed Rail System?" The Atlantic's City Lab, August 13, 2014, http://www.citylab.com/politics/2014/08/why-cant-the-united-states-build-a-high-speed-rail-system/375980/.

[8] Marc H. Burns, *High-Speed Rail in the Rear-View Mirror: A Final Report of the Texas High-Speed Rail Authority* (Austin, Texas: MH Burns, 1995).

[9] Batheja and Smith, "The Bullet Train that Could Change Everything."

Figure 1. Dallas-Houston HSR County Map with Recommended Alternatives




Source: "Dallas-Houston High Speed Rail County Maps," Federal Railroad Administration, accessed October 5, 2015, https://www.fra.dot.gov/eLib/Details/L16213.

High-speed trains have developed sophisticated approaches to reducing threats from natural disasters and conditions. Japanese trains, engineered with earthquakes in mind, all came to a safe stop during the 2011 Fukushima disaster without loss of life or serious injury.[10] There is one known instance of a high-speed train in England derailing

[10] Nobuo Mimura et al., "Damage from the Great East Japan Earthquake and Tsunami: A Quick Report," *Mitigation and Adaptation Strategies for Global Change* 16, no. 7 (2011): 803–818. 7.

with loss of life; the cause was rail fatigue.[11] A 2013 high-speed train crash in Spain was the result of human error.[12] However, there is a long and growing list of fatalities and injuries from terrorist attacks against passenger transportation systems including intercity high-speed trains. The possibility has been raised by area residents: the Commissioners Court of Grimes County, Texas has gone on record opposing the project, listing five main objections, including increased risk of terrorist attacks.[13] A real estate broker asked in a public scoping meeting for the project's environmental impact study if the "bullet train is bullet proof?"[14]

In fact, there are serious concerns about how the project sponsors will address the potential for acts of terrorism. These concerns stem from instances around the world as well as the specifics of the TCR project. Barkakarti and Maurer calculated that "from January 2004 through July 2008 there were 530 terrorist attacks worldwide against passenger rail targets, resulting in more than 2,000 deaths and 9,000 injuries."[15] The Transportation Safety Administration (TSA) considers passenger railroads to be:

> High consequence targets in terms of potential loss of life and economic disruption as they carry large numbers of people in a confined environment, offer the opportunity for specific populations to be targeted at particular destinations, and often have iconic structures.[16]

---

[11] M. Kameswara Reddy et al., "Stress Analysis on Behaviour of Rails," *International Journal of Engineering Research* 4, no. 1 (2015): 4–8. http://works.bepress.com/cgi/viewcontent.cgi?article=1431&context=irpindia.

[12] Lucas Laursen, "Spanish High-Speed Train Crash Offers Safety-System Lessons," *Scientific American*, July 26, 2013, accessed December 28, 2014, http://www.scientificamerican.com/article/ish-high-speed-train-crash/.

[13] "County, Anderson Officially Oppose Bullet Train," *The Navasota Examiner*, last modified January 14, 2015, accessed November 14, 2015, http://www.navasotaexaminer.com/news/article_1fef694c-9c13-11e4-a952-976fd25da9c2.html.

[14] "County Judge-Elect Leads Charge to Derail Bullet Train," *The Navasota Examiner*, last modified December 10, 2014, accessed November 14, 2015, http://www.navasotaexaminer.com/news/article_7d0e59e2-7ffa-11e4-a057-eb71e891d34d.html.

[15] Nabajyoti Barkakati, and David Maurer, *Technology Assessment: Explosives Detection Technologies to Protect Passenger Rail* (Washington, DC: Government Accountability Office, 2010).

[16] 73 Fed. Reg. 72130 (2008).

TCR clearly falls into this category because, along with other aspects, it will have iconic structures.[17] Further, there is international precedent for attacks on high-speed trains. Between 1970 and 2012 worldwide, there were 33 high-speed rail attacks, which killed 32 people.[18] However, in 40 years, there has only been one death involving a U.S. train that could be ascribed to a terrorist action, a 1995 incident derailing Amtrak's Sunset Limited.[19] Also, one school of thought is that an initially high threat level due to HSR newness will subside over time.[20]

Like other high-speed trains, the TCR system will accomplish the movement of people through physical rail cars over rails. Terrorist attacks on passenger rail systems include Madrid in 2004, London in 2005, Mumbai in 2006, and Kunming in 2014. The French HSR line is fenced (as TCR's will be) but in 1995, saboteurs penetrated the fence and planted a bomb which failed to explode.[21]

Cyber systems such as train control and electronic aspects like online ticketing require sophisticated security precautions. Protections for rail systems, even those with sophisticated electronic protections, can be defeated by people who already have access. A number of examples appear later in this thesis.

This writing was prepared using publicly available information. None of the materials used were classified or labeled "For Official Use Only" or "Law Enforcement Sensitive." This approach allows for the broadest dissemination of the information of this writing but brings with it two key limitations.

The first limitation is that the proposed project is private sector-driven. The project developer expects the plans to change over time. Certain details of the project are

---

[17] Nicholas Sakelaris, "High-Speed Rail Station Will be 'Iconic' Part of Dallas Skyline, CEO Says," *Dallas Business Journal*, November 21, 2014.

[18] Brian Michael Jenkins et al., *Formulating a Strategy for Securing High-Speed Rail in the United States* (San Jose, CA: Mineta Transportation Institute, 2013), 9.

[19] Ibid.

[20] Ibid.

[21] Brian Michael Jenkins, Bruce R. Butterworth, and Jean-Francois Clair, *The 1995 Attempted Derailing of the French TGV (High-Speed Train) and a Quantitative Analysis of 181 Rail Sabotage Attempts* (San Jose, CA: Mineta Transportation Institute, 2010).

proprietary and thus have not been released. For example, the company has not released any ridership studies, nor is it required to at this point. Therefore, it is necessary that this writing rely on published reports regarding the proposed project from sources that include the company, its participants and sponsors, public reports from relevant government agencies, magazine and news articles (including online publications), observers, and other interested parties. A study by the RAND Corporation, which specifically examined publicly available information about transportation infrastructure in order to assess vulnerabilities, found "the utility and comprehensiveness of information available in the public domain varies by infrastructure and scenario."[22] In New York, a red team exercise based on a scenario where terrorists attempt to bomb a commuter train, based on the Madrid incident, planners "did not find any publicly available data suggesting there are any countermeasures in place to thwart the attack scenario…."[23]

The second limitation is that a number of government agencies have been, are, or will be involved in the proposed train project. There are at least a dozen federal agencies and three state agencies involved in the environmental impact study alone.[24] Inherently, publicly released government information in the security area is limited. There is no requirement that either the government or the private sector release information regarding security considerations for a private sector project. The possibility that security considerations merit a public discussion, while controversial, has taken place in other arenas. For example, some have argued that environmental impact statements for nuclear power plants should address the potential environmental effects of a terrorist attack.[25] That particular conversation has led to multiple lawsuits and conflicting legal rulings. As things currently stand, there is no such federal requirement for public review, and an exposition and analysis of the costs and benefits as far as critical transportation infrastructure is concerned is beyond the scope of this writing.

---

[22] Eric Landree et al., *Freedom and Information: Assessing Publicly Available Data regarding U.S. Transportation Infrastructure Security* (Santa Monica, CA: Rand Corporation, 2007).

[23] Ibid., 68.

[24] Federal Railroad Administration, *Dallas to Houston High-Speed Rail Environmental Impact Statement: Scoping Report* (Washington, DC: Federal Railroad Administration, 2015).

[25] Amanda Mott, "Should the Threat of a Terrorist Attack on a Nuclear Power Plant be Considered Under NEPA Review," UCLA Journal of International Law and Foreign Affairs 12 (2007): 333.

The TCR project is unlike any other in this country but shares some aspects of existing transportation approaches. Like airlines and intercity buses, it is privately owned. Like public-sector commuter rail systems, it is a steel wheel on steel rail train, and like some passenger trains in the Northeast Corridor, it is powered by electricity from overhead wires.

This proposal brings with it an array of unique and unprecedented homeland security issues. Train bombings in Madrid and London, the Aum Shinrikyo episode in Japan, and attacks on high-speed trains elsewhere raise questions about the security of passenger rail transportation. A modern high-speed rail system is a network of potential vulnerabilities, and terrorist groups have identified public transportation as desirable targets. The train set with its passenger load is both a physical target and a symbolic target—an attack could be a statement against wealth or foreign investment, and would likely result in considerable media coverage. There are hundreds of miles of right-of-way[26] and track structures, including intermodal stations, maintenance facilities with train storage areas, and the physical grid that provides electricity to power the trains. Train control, financial, ticketing, and other back-end systems are potential cyber targets. Train control systems are the biggest element in the system's safety plan and pose a large security threat. To address threats effectively, this particular project should be integrated with law enforcement, especially intelligence. Consequences of failure to anticipate and protect the train system range from financial loss to fatalities, immediate and long-term injuries, and symbolic victories for terrorist entities.

Through the Transportation Security Administration, the federal government has security oversight for passenger rail systems. Its approach for rail is similar to that for intercity buses as opposed to the screening and security levels provided for air transportation. Passenger rail receives minimal security oversight from the state level. Local rail systems are public entities and provide their own security or rely on police agencies.

[26] The term "right of way" is used in this thesis to mean the entirety of the land TCR will own or use for the path of the train.

Short of statutory change, the state does not appear to have the ability to impose any security standards or requirements on the project. Should the train operators be required to participate in intelligence-gathering efforts? Is it in the state's interest to mandate a level of law enforcement presence, either on board the train or at stations? Will financial backers of the Texas Central Railway (TCR) system require security standards, both as a means of protecting the asset and its ability to generate revenue to repay its debts?

This rail project raises many questions that merit attention and review.

- Given the unique nature of the project, should government's oversight role change?
- What homeland security factors should be considered as this private sector project moves forward?
- Should there be a required analysis, as part of the National Environmental Policy Act review or freestanding?
- Are there or should there be roles for federal, state, and local government regulation, participation, or oversight?
- If not a direct role, are there impacts that these agencies would be advised to prepare for?
- Are the methods used in the Northeast Corridor and elsewhere applicable to this project, or does its higher speed, privatized nature, geography, or approach require different methods?
- What are the expectations for privacy if the railroad provides Wi-Fi and cell phone coverage?
- What are the implications of heavy foreign investment and involvement?

My hypothesis is that the State of Texas should require homeland security standards for high-speed rail. These standards would provide a baseline set of requirements for projects of this nature, and could include precedents for how law enforcement is achieved; how the project leaders interact with the intelligence community; considerations regarding cyber security; passenger privacy, vulnerability, and threat assessment; and participation in planning committees. This topic will be of interest to an audience of policymakers, homeland security practitioners, and possibly

even the project developers. It provides some flexibility so that if this project should cease, the research would lay the groundwork for a paradigm applicable to future projects.

The following chapters describe the proposal in more detail, providing historical information about terrorist incidents affecting rail transit generally as well as high-speed intercity passenger rail specifically. The various chapters identify and discuss vulnerabilities and threats, frame the legal context, compare possible approaches, and make recommendations for further action.

THIS PAGE INTENTIONALLY LEFT BLANK

# II. LITERATURE REVIEW

## A. THE STATUS OF RESEARCH, GENERALLY

Seven universities house federally-supported centers of transportation security excellence. These centers are charged with a broad area of transportation-related security issues, including threat identification, resilience, policy, and training.[27] However, with a few exceptions, there are few publications emanating from these institutions regarding potential high-speed intercity rail implementations in the U.S. and, in particular, very few if any that are specific to the TCR project.

The major public entity with a high-speed rail security focus is San Jose State University's Mineta Transportation Institute. The major private, nonprofit entity is the RAND Corporation. A key author, Brian Michael Jenkins,[28] is associated with both. This focus is logical, given that they are both headquartered in California, which has had a state-level authority attempting to implement a high-speed rail project since 1996. Jenkins appears to be the most prolific author in this area.[29] His works, cited by hundreds (according to Google Scholar), appear to be comprehensive, thoroughly researched, and consistent with other studies in the area. There is one notable exception; Jenkins alone has theorized that any threat to high-speed rail above any other commuter rail will subside when the newness wears off.[30]

---

[27] "National Transportation Security Center of Excellence," Department of Homeland Security, Office of University Programs, accessed December 7, 2014, https://ntscoe.hsuniversityprograms.org/centers-of-excellence/ntscoe/.

[28] Brian Michael Jenkins, "About—Brian Michael Jenkins," accessed December 7, 2014, http://www.brianmichaeljenkins.com/about/.

[29] Jenkins, Butterworth, and Clair, *The 1995 Attempted Derailing of the French TGV*; Brian M. Jenkins, and Joseph Trella *Carnage Interrupted: An Analysis of Fifteen Terrorist Plots against Public Surface Transportation* (San Jose, CA: Mineta Transportation Institute, 2012); Brian M. Jenkins, *Terrorism and the Security of Public Surface Transportation* (Santa Monica, CA: RAND Corporation, 2004); Brian M. Jenkins, and Bruce R. Butterworth, "Mineta Transportation Institute Says Subways are Still in Terrorists' Sights," *PRN Newswire*, March 24, 2014, accessed December 7, 2014, http://www.prnewswire.com/news-releases/mineta-transportation-institute-says-subways-are-still-in-terrorists-sights-252015231.html.

[30] Brian Michael Jenkins et al., *Formulating a Strategy for Securing High-Speed Rail in the United States* (San Jose, CA: Mineta Transportation Institute, 2013), 14.

There are a wide range of academic studies that are applicable to high-speed rail as a part of a larger mass transportation network. For instance, Michael Greenberg of Rutgers University works in this area.[31] Like Virginia Tech's Pamela Murray-Tuite[32] and Sunniva Meyer of the Institute of Transport Economics in Oslo, Norway,[33] Greenburg identifies aspects of transportation security that can be mathematically modeled, thus projecting likely outcomes when the inputs are varied. Meyer uses a prisoners' dilemma-like approach, which is broadly applicable. The studies of both Greenberg and Murray-Tuite would need their variables to be adjusted to local conditions to be directly applicable. Many other studies address high-speed rail but do not take up security issues.

One report, a graduate paper titled "High-Speed Rail in the US: Will It Be a More Attractive Terror Target than Inter-city Rail?,"[34] is recent and on point, except it is not specific to Texas or Japan. However, it contains sensitive information so while its usefulness in this writing, intended to be open source, is limited, it can be evaluated within the context of the research.[35]

## B. SUBGENRES

Subgenres include the record and practice in Japan, high-speed rail security as implemented and experienced elsewhere in the world, general protection of critical

---

[31] Michael Greenberg et al., "Passenger Rail Security, Planning, and Resilience: Application of Network, Plume, and Economic Simulation Models as Decision Support Tools," *Risk Analysis* 33, no. 11 (2013): 1969–1986.

[32] Pamela M. Murray-Tuite, and Xiang Fei, "A Methodology for Assessing Transportation Network Terrorism Risk with Attacker and Defender Interactions," *Computer-Aided Civil and Infrastructure Engineering* 25, no. 6 (2010): 396–410.

[33] Sunniva F. Meyer, "Preventing Mass Killings: Determining the Optimal Allocation of Security Resources between Crowded Targets," *Peace Economics, Peace Science and Public Policy* 17, no. 1 (2011).

[34] Donna R. Maurillo, "High-Speed Rail in the US: Will it be a More Attractive Terror Target than Inter-City Rail?" (master's thesis, San Jose State University, 2012).

[35] The report carries this statement: "Some of these materials, especially those related to law enforcement alerts or other security-sensitive resources, have been designated as unclassified but for official use only (U/FOUO). Access has been given to this researcher by security sources with the understanding that any U/FOUO information made available to the public will be used only in aggregate. In any instances where U/FOUO documents have been quoted or made identifiable in this report, they have been identified as such."

infrastructure along with and key resources, security for transportation under both public and private sectors, and unique aspects of this particular proposed project.

### 1. Transportation Security in the United States

A significant body of work is available regarding transportation security in the United States. Approaches used by various authors include looking at the subject from the perspectives or particular interests involved in mass transit, critical infrastructure, and natural and man-made disasters. Authors who have taken a position are in general agreement that "airline-style" security is inappropriate for trains because it would reduce or eliminate trains' usefulness[36] or be no more than "security theater."[37]

Transportation and passenger security are well covered in a series of studies from the Congressional Research Service (CRS), the Department of Homeland Security (DHS), Government Accountability Office (GAO), and others.[38] These tend to be generic or lean towards commuter rail. As *Mass Transit Magazine*'s Kim Kaiser notes (citing Brian Jenkins),[39] there are important differences between the two, such as the HSRs have more kinetic energy at speed and are constructed above ground.

### 2. Unique Aspects of the Proposed Project

The recent and unprecedented nature of the proposed project limits scholarly research to the project developer's formal submissions to the state and federal governments, the developer's public-facing website, statements, and representations, and media articles. The developer's representations are of questionable value as they carry the disclaimer:

---

[36] Brian D. Taylor, "Terrorist Attacks and Transport Systems," *ACCESS Magazine* 1, no. 28 (2006).

[37] Michael Scott Moore, "High-Speed Rail's Weak Link is Security," *Pacific Standard*, May 4, 2011, accessed October 27, 2014, http://www.psmag.com/navigation/politics-and-law/high-speed-rails-weak-link-is-security-30874/.

[38] For example David R. Peterman, Bart Elias and John Frittelli, *Transportation Security: Issues for the 111th Congress* (Washington, DC: Congressional Research Service, 2009); Patrick O'Malley, *TSA's Preparedness for Mass Transit and Passenger Rail Emergencies* (Washington, DC: U.S. Department of Homeland Security, Office of the Inspector General, 2010).

[39] Kim Kaiser, "High-Speed Rail Security Needs a Different Approach than Commuter Rail," *Mass Transit Magazine*, August 11, 2011, accessed December 8, 2014, http://www.masstransitmag.com/article/10317151/high-speed-rail-security-needs-a-different-approach-than-commuter-rail.

> All claims and descriptions of the high-speed rail system's operations, including service and station amenities, are solely suggestions of potentiality based on examples from other high-speed rail around the world and for promotional purposes only. TCR will not be the owner, developer, implementer nor operator of the railroad. The railroad's owner or operator will be responsible for coordinating with regulatory agencies and others regarding the specific aspects of the system's service.[40]

Documents submitted by or to the state and federal governments in association with the environmental impact statement, found on a dedicated website,[41] are more reliable due to the legal requirements of the National Environmental Policy Act. It is possible that some of the information may become available after environmental clearance is achieved. The corporation's priorities are likely to be oriented first toward resolving legislative concerns and getting contracts in place for design-build construction, train equipment/rolling stock, and operating and maintenance contracts (O&M)—all necessary to provide hard numbers for their financial plans and debt/equity offerings. Second, TCR will be working out its safety system plan with the Federal Railroad Administration (FRA). This plan might provide a nexus for security concerns (e.g., how TCR will protect the train control systems that ensure safety) in addition to standard rail safety concerns as they may apply to a trainset and system not currently in operation in this country (e.g., details about the vehicle construction, such as window glazing). News and web-based media may have information unavailable elsewhere due to interviews or research, but so far, they have rarely provided much insight into the details of the project itself. This may be as much a function of the details not having yet been decided, as them having been decided but not being available.

### 3. High-Speed Rail Security Issues around the World

In addition to the aforementioned works, several authors have produced reviews or analysis of high-speed rail and terrorism or security issues. For instance, Francesca De

[40] David Benzion, "Texas Central Railway," Texas Central Railway, accessed September 21, 2014, http://texascentral.com/.

[41] Michael Johnsen, "Dallas to Houston High-Speed Rail—Passenger Service from Houston to Dallas," Federal Railroad Administration, accessed September 21, 2014, https://www.fra.dot.gov/Page/P0700.

Cillis analyzed 540 criminal and terrorism related incidents on passenger rail (not limited to high speed rail) to find key similarities and project high vulnerabilities. She concludes that stations are the most likely targets and with attacking such venues that higher body counts can be expected.[42] Dylan Kissane produced an excellent analysis of terrorism and the French high speed train.[43] There is not much agreement among authors as to whether the station, the trainset itself, or the right-of-way is the most vulnerable aspect of a high-speed rail system. This area requires further analysis and thought, and the answer is likely to vary depending on the design of these aspects and the capabilities of those who would pose a threat. This writing engages a systematic approach to discussing vulnerabilities in relation to potential threat vectors.

### 4. What is the Real Japanese High-Speed Train Safety Record?

Information about the true safety and security record of Japanese trains is hard to come by, which may be a result of the privatized nature of the Japanese rail system. Some discussions about Japanese high-speed rail omit safety altogether, claim no fatal accidents,[44] or give it only a cursory treatment. In a 2012 presentation, a senior official of Japan's Ministry of Land, Infrastructure, Transport and Tourism railroad department gave a 34-slide PowerPoint presentation. In it, the safety slide discussed train control and gave one sentence pertaining security: "Fatalities to date: ZERO for 47 years since the start of operation in 1964."[45] The rest of the presentation is wholly positive about the train, suggesting the national agency is more protective of this technology and participating in its marketing to other countries than it is interested in balance.

This zero fatalities claim is qualified, however, by the Central Japan Railway Company in its online material as "no passenger fatalities or injuries due to train

---

[42] Francesca De Cillis et al., "Analysis of Criminal and Terrorist Related Episodes in Railway Infrastructure Scenarios," *Journal of Homeland Security and Emergency Management* 10, no. 2 (2013): 447–476.

[43] Dylan Kissane, "Terror on the TGV? The Terrorist Threat to France's High Speed Train Network," (Paris: Centre d'Etudes Franco-Americain de Management, 2007).

[44] Inaki Barron, "50 Years of High Speed Rail," *UIC e-News*, no. 418, October 7, 2014, International Union of Railways, accessed December 7, 2014, http://uic.org/com/uic-e-news/418/.

[45] Akihiko Tamura, *An Overview of Japan's High Speed Rail: Shinkansen* (Tokyo, Japan: Ministry of Land, Infrastructure, Transport, and Tourism, 2012), 10.

accidents such as derailment or collision in commercial train operations during 47 years of service."[46] JRC's material online is extensive but the safety and security portions are focused on mechanical issues and earthquakes.

Figure 2 shows the Shinkansen N700-I in a multitrack urban setting with gantries providing overhead electrical service. Figure 3 shows it with two tracks in a rural setting.

Figure 2. Shinkansen N700-I in Multitrack Urban Setting

Source: "Shinkansen N700-I," Railway Technology, accessed October 5, 2015, http://www.railway-technology.com/projects/n700-shinkansen/n700-shinkansen1.html.

[46] "Safety," Central Japan Railway Company, accessed December 7, 2014, http://english.jr-central.co.jp/about/safety.html.

Figure 3. Shinkansen N700-I In Rural Two-track Configuration

Source: "JR Central/JR West N700 Series," *Japan Times*, September 27, 2014, accessed October 5, 2015, http://jto.s3.amazonaws.com/wp-content/uploads/2014/09/p14-schreiber-shinkansen-g-20140928-870x489.jpg.[47]

Even though Japanese high-speed trains are integrated into the overall passenger rail system, a 1995 sarin gas terrorist incident that resulted in 12 fatalities and thousands injured occurred in the subway, not in the high-speed rail portion.[48] In addition, a man who set fire to himself as a political protest in 2014 did so outside the Shinjuku railway station, and the incident had no impact on high-speed train operations or passengers. JRC's website also reveals that two unexploded bombs, apparently U.S. Navy ordnance dating from World War II, have been found at the high-speed train factory, and that travel schedules were disrupted when the bombs were disposed of.[49]

Jenkins of the Mineta Institute found four Shinkansen fatalities: three suicides by people jumping from trains and one death of a passenger caught in a train door.[50] If one

[47] The article by Mark Schreiber, "Shinkansen at 50: Fast Track to the Future," that accompanies the image can be found at: http://www.japantimes.co.jp/life/2014/09/27/lifestyle/shinkansen-50-fast-track-future/#.VhL0Dyuq2VA.

[48] Jason Testar, "What Tokyo Taught Us," *Homeland Defense Journal* 1, no 3 (June: 2003): 34–39.

[49] Central Japan Railway Company, *The Effect of Bomb Disposal at the Hamamatsu Workshop Site on Train Service* (Tokyo, Japan: Central Japan Railway Company, 2012); Central Japan Railway Company, *The Effect of Bomb Disposal at the Hamamatsu Workshop Site on Train Service* (Tokyo, Japan: Central Japan Railway Company, 2013).

[50] Jenkins et al., *Formulating a Strategy for Securing High-Speed Rail in the United States*, 50.

assumes the train was operating properly in the case of the train door death, the JRC's qualified statement would be accurate. However, any blanket "zero fatalities" statement would not, and other questions would be raised about how the issue was accounted for and resolved. However, the Mineta report does not cite or source the statement in question, so an exact answer is elusive.

In June of 2015, a man set himself on fire inside a JRC Tokyo-to-Osaka high-speed train, killing himself and a passenger and injuring 26 people, mostly from smoke inhalation.[51] It remains to be seen how this incident will be represented in safety materials going forward.

## C. CONCLUSION

Working from the general (transportation security) to the specific (security implications of the proposed Texas project), the research field appears like an inverted pyramid. At its widest is a vast range of literature chronicling historical terrorism on transportation facilities. In the middle are academic analyses quantifying various aspects and using the results to identify possible vulnerabilities or recommend actions. As the field is narrowed to HSR and then HSR in the U.S., a few authors and sources become prominent. In some instances, more research is needed to provide a basis to determine credibility. At the exact point this writing examines, it appears that this work is the first of its kind.

[51] "Man Sets Self on Fire on Japanese Bullet Train, Killing Himself and 1 Other," New Europe, accessed October 29, 2015 http://neurope.eu/wires/man-sets-self-on-fire-on-japanese-bullet-train-killing-himself-and-1-other.

# III. MAJOR COMPONENTS

DHS has contracted with the Argonne National Laboratory[52] to create a framework for use in evaluating site security for the DHS Enhanced Critical Infrastructure Protection Program.[53] The framework lists six major components: Security Management, Physical Security, Information Sharing, Security Force, Dependencies, and Protective Measures.[54]

These major components combined have 42 subcomponents. Table 1 lists the major components and their subcomponents.

Table 1. Major Components and Subcomponents for Measuring Vulnerability (Argonne National Laboratory)

| |
|---|
| 1. Physical Security |
| Access control |
| Fences |
| Gates |
| Closed-circuit television (CCTV) |
| Intrusion detection system (IDS) |
| Parking |
| Lighting |
| Vehicle access control |
| Building envelope |
| 2. Security Management |
| Business continuity plan |
| Security plan |
| Emergency action plan |
| Threat levels |
| Security information communication |
| External security exercises |
| Executive protection program |

[52] "Better Infrastructure Risk and Resilience," Argonne National Laboratory, last modified August, 2010, accessed October 6, 2015, http://www.anl.gov/articles/better-infrastructure-risk-and-resilience.

[53] "ECIP: Homeland Security," Department of Homeland Security, last modified September 9, 2015, accessed October 6, 2015, 2015, http://www.dhs.gov/ecip.

[54] Robert E. Fisher et al., Constructing Vulnerability and Protective Measures Indices for the Enhanced Critical Infrastructure Protection Program (No. ANL/DIS-09-4), (Argonne, IL: Argonne National Laboratory, 2009), http://www.osti.gov/scitech/biblio/966343.

| | |
|---|---|
| | Security working groups |
| | Sensitive information identified |
| | National security clearance |
| | Background checks |
| 3. | Security Forces |
| | Staffing |
| | Equipment/weapons |
| | Training |
| | Post guidelines |
| | Patrols |
| | Random patrols |
| | After hour security |
| | Checks recorded |
| | Command and control |
| | Memorandum of understanding (MOU)/memorandum of agreement (MOA) |
| 4. | Information Sharing |
| | Threat sources |
| | Information sharing mechanisms |
| 5. | Protective Measures Assessment |
| | New protective measures |
| | Random security measures |
| 6. | Dependencies |
| | Critical products (chemicals, fuels, raw materials, packaging, medical supplies, feed, and by-products/waste) |
| | Electricity |
| | Information technology (Internal and Internet business, and internal and Internet control) |
| | Natural gas |
| | Telecommunications (telephone, data, and radio link) |
| | Transportation rail, air, road, maritime, and pipeline |
| | Water |
| | Wastewater |

Adapted from Fisher et al., "Constructing Vulnerability and Protective Measures Indices," 4.

This list provides a good set of constructs from which to draw. For the purposes of a fault tree analysis, we will use these measures for our framework. Subsequent sections address each major component in more detail through the consideration of subcomponents. Moreover, specific subcomponents have been selected for analysis due to the need for brevity and manageability.

## A. PHYSICAL SECURITY

Protecting a train system involves anticipating where someone might try to attack or breach the system and addressing those points. System entry can be accomplished using human vectors (insiders or people who inadvertently or maliciously allow a defensive measure to be defeated), cyber vectors (computer-based intrusions), and breaches of a physical item like a building or fence.

### 1. Introduction

Intercity passenger train systems have three main physical components: the stations (nodes), the trainset itself, and the right-of-way (including maintenance facilities). Each component has subsets that operate in the background, including electric grid, communication, and cyber systems.

Texas Central Railway (TCR) has stated that it intends to use N700-I,

> The international version of the Tokaido Shinkansen total system currently in operation between Tokyo and Osaka, Japan. This international version will feature the core system—passenger train, overhead catenary, tracks, signaling—along with all of the corresponding maintenance and operations protocols that have made Tokaido Shinkansen operations so safe, efficient and successful for nearly 50 years.[55]

The Central Japan Railway Company (JRC), a participant in TCR, represents that this holistic approach to the physical system is essential in providing a safety record similar to that experienced in Japan. Implementing this project as a holistic, integrated unit allows coordinating the track and trainset to optimize the geometry and physical interaction. According to a company presentation, JRC "has secured the safety and the high quality of the Tokaido Shinkansen through the integrated management of both the hardware and software that make up the system."[56] The physical system is a network of networks, a system of systems, designed from the ground up to function well as a unit,

---

[55] David Benzion, "The Facts," Texas Central Railway, accessed September 21, 2014, http://texascentral.com/the-facts/.

[56] Tsutomu Morimura, *Introduction of the N700-I Bullet* (Nagoya, Japan: Central Japan Railway Company, 2010).

which should provide greater service than separately produced systems at the cost of sole source acquisition and increased expense.[57]

The proposed high-speed rail system is an electric steel wheel on steel rail passenger train system that is a fully fenced and grade separated. The N700-I is designed for each train to consist of at least six passenger cars, up to 15 passenger cars, in which every axle is powered, with a non-passenger car on each end. The maximum cruising speed is 205 miles per hour (330 kilometers per hour).[58] The train will connect Dallas and Houston—about 250 miles (400 kilometers)—and take about 90 minutes, with trains running at 30-minute intervals at the outset.[59]

In addition, TCR has indicated there will be at least one multimodal station (node) in Dallas and one in Houston, and at least one intermediate station, located in Shiro; however, the locations of any maintenance facilities are only speculative at this point.

In terms of vulnerabilities and threats, Wilson and others from the RAND Corporation examined over 800 terrorism incidents in the rail transportation arena around the world.[60] They found that about three fourths of the attacks involved physical infrastructure and were intended to hurt passengers. These attacks were on the rail itself, the interior of train cars, and stations.[61] Additionally, one fourth of the attacks were at stations, one fourth inside train cars, and one fourth on tracks. Seventeen percent were on the outside of train cars, five percent on supporting infrastructure, four percent on areas outside of stations, and three percent on equipment (any errors are due to rounding).

---

[57] Dianna Wray, and Eric Nicholson, "What Will a Bullet Train Mean for the Future of Texas?" *Houston Press*, last modified August 18, 2015, accessed October 8, 2015, http://www.houstonpress.com/news/on-the-line-will-the-houston-dallas-bullet-train-revolutionize-texas-or-divide-it-forever-7679365.

[58] Morimura, *Introduction of the N700-I Bullet*, 5.

[59] Scott Dixon, "Texas to Get Shinkansen System," *The Japan Times*, August 2, 2014, http://www.japantimes.co.jp/news/2014/08/02/business/economy-business/private-u-s-railway-wants-bullet-train-line-for-texas-by-2021/#.VB7cHhZ_TYQ.

[60] Jeremy M. Wilson, *Securing America's Passenger-Rail Systems* (Santa Monica, CA: Rand Corporation, 2007).

[61] Ibid.

### 2. Passenger and Baggage Screening

The intersection of the stations and trainsets is the point where passengers board trains. The Texas Legislature may take an interest in this particular point of vulnerability and the question of whether passengers and their carry-on luggage receive the kind of scrutiny that those at airports do. (At this writing, the U.S. Coast Guard is proposing that cruise ships begin using screening procedures similar to airports.)[62]

This discussion generally views "airport-style security" as the kind that takes place at commercial aviation airports. There are other kinds of aviation with different approaches to security in particular general and business aviation—privately owned, corporate leased, or that otherwise running on a different security structure. General aviation airports alone account for 3000 airports, the largest slice of the U.S. airport pie.[63] Industry,[64] federal,[65] legislative,[66] and executive[67] agencies, and states[68] have invested a great deal of study in general aviation as well.

Aviation security is sometimes part of a larger discussion about homeland security and related issues. For example, when Congress passed the REAL ID act,[69]

---

62 "Cruise Ships Face Airport-Style Security Measures," The Hill, last modified December 9, accessed November 15, 2015, http://thehill.com/regulation/226514-cruise-ships-facing-new-airport-like-security-measures.

63 "General Aviation Airports Report—Airports," Federal Aviation Administration, last modified March 19, 2014, http://www.faa.gov/airports/planning_capacity/ga_study/.

64 For example, "General Aviation Security Information for Journalists, Aircraft Owners and Pilots Association," accessed December 6, 2015, http://www.aopa.org/Media-Relations/Position-Papers/General-Aviation-Security.aspx.

65 For example, "Aviation Security," Department of Homeland Security, last modified September 23, 2015, http://www.dhs.gov/general-aviation.

66 For example, "GAO Report on General Aviation Security Risks, Airports Council International-North America," accessed December 6, 2015, http://www.aci-na.org/content/gao-report-general-aviation-security-risks.

67 For example, Transportation Security Administration, *Security Guidelines for General Aviation Airports* (Information Publication A-001), (Washington, DC: Transportation Security Administration, 2004), https://services.oregon.gov/aviation/docs/guidelines_for_ga_airports.pdf.

68 For example, *General Aviation Security* (National Association of State Aviation Officials, Silver Spring, MD, 2002), http://www.state.nj.us/transportation/airwater/aviation/pdf/nasao.pdf.

69 "REAL ID Act—Title II, H.R.1268, Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005 (Enrolled as Agreed to or Passed by Both House and Senate), accessed December 6, 2015, http://www.dhs.gov/xlibrary/assets/real-id-act-text.pdf.

states were expected to change their driver license and state-issued identification processes to comply. Several states either asked to postpone compliance with the various provisions of REAL ID or, in some instances, refused to participate. In response, those states were told their driver licenses and state issued identification would not be recognized at airports and, if enforced, would deny their citizens access to commercial airliners.[70]

In Texas, there is precedent for state legislative involvement in commercial aviation. The Dallas-Fort Worth Airport is essentially a joint local government.[71] State legislative activity paved the way for the federal repeal of the Wright Amendment,[72] enabling long distance direct flights from Dallas Love Field.[73] More recently, the Texas Legislature has focused on what some perceive as intrusive examinations at airports. In 2011, the Texas Legislature considered legislation that would essentially subject TSA personnel to a charge of official oppression if they touched a passenger.[74] The bill saw passage in the House but stalled in the upper chamber when the federal government threatened to restrict interstate flights, citing security reasons.[75] In 2013, Texas attempted to create a Security Screening Opt-Out Program, but the legislation did not pass.[76] In 2015, the legislature passed a resolution asking Congress to require the TSA to accept a

---

70 Daniel C. Vock, "Feds Push Gently on 'REAL ID,'" Pew Trusts, January 22, 2014, http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2014/01/22/feds-push-gently-on-real-id.

71 "DFW Airport Administration," Dallas/Fort Worth International Airport, accessed December 6, 2015, https://www.dfwairport.com/about/admin/index.php.

72 N. B. "The Wright Amendment: Good Riddance," *Gulliver* [*The Economist* blog], December 12, 2014, http://www.economist.com/blogs/gulliver/2014/12/wright-amendment.

73 *The Wright Amendment, Hearing before the Subcommittee on Aviation of the Committee on Commerce, Science, and Transportation, United States Senate*, 109th Cong. (2005), http://www.gpo.gov/fdsys/pkg/CHRG-109shrg62992/html/CHRG-109shrg62992.htm.

74 "House Bill 1937, Texas Legislative Council," 2011, accessed December 6, 2015, http://www.legis.state.tx.us/BillLookup/Text.aspx?LegSess=82R&Bill=HB1937.

75 Mac Slavo, "Feds Threaten Texas with No-fly Zone over Anti-TSA Legislation," SHTFPlan, May 25, 2011, http://www.shtfplan.com/headline-news/feds-threaten-texas-with-no-fly-zone-over-anti-tsa-legislation_05252011.

76 "House Bill 1719," Texas Legislative Council, 2013, accessed December 6, 2015, http://www.legis.state.tx.us/BillLookup/History.aspx?LegSess=83R&Bill=HB1719.

Texas concealed handgun license as a form of official identification,[77] but as of this writing, the TSA does not allow any weapons license to serve as proper identification.[78]

The literature generally provides little guidance in this area. A RAND study found the most Europeans do not like having their person or bags searched, preferring faster and less intrusive security measures, such as cameras and security personnel.[79] An independent Australian review of aviation security notes malfunctioning machinery at certain airport security stations but does not suggest that the problem is widespread or significant. Speaking about Australian general aviation airports, John Wheeler reported,

> Unmanned, undermanned, or poorly-equipped access points to restricted areas both inside and outside terminals clearly represent weak spots. Abuse, misuse, or false use (including tailgating) can occur with obsolete or unsophisticated swipe-card systems. A thorough inspection for contraband of the contents of each vehicle entering and leaving the secure area would prove oppressively expensive, and probably so time-consuming that airport functioning would be seriously impaired.[80]

However, he offers no recommendations in this area. In *Comparative Homeland Security*, Morag concisely describes the three different types of regulated airports in Australia as well as the unregulated general aviation airfields and notes the great variation in passenger screening among them.[81] A representative of airline pilots, quoted in *The Myth of Security at Canada's Airports*, suggests more emphasis should be placed on screening of employees and others with access to airplanes than on screening passengers.[82] In a

---

77 "House Bill 1215," Texas Legislative Council, 2015, accessed December 6, 2015, http://www.legis.state.tx.us/BillLookup/history.aspx?LegSess=84R&Bill=HR1215.

78 "Identification," Transportation Security Administration, accessed December 6, 2015, http://www.tsa.gov/travel/security-screening/identification; Luke McCoy, "Did You Know That Your Texas Concealed Handgun License is Now a Valid Proof of Identification?" USA Carry, September 23, 2015, http://www.usacarry.com/texas-concealed-handgun-license-valid-id/.

79 Sunil Patil et al., "Privacy Vs Security?" *RAND Europe Research Brief* (2015). http://www.rand.org/pubs/research_briefs/RB9843z1.html.

80 John Wheeler, and John D. L. Wheeler, *An Independent Review of Airport Security and Policing for the Government of Australia* (Canberra: Department of Transport and Regional Services, 2005), 49.

81 Nadav Morag, *Comparative Homeland Security: Global Lessons* (Wiley Series on Homeland Defense and Security), (Hoboken, NJ: John Wiley and Sons, 2012), Kindle location 5892.

82 *The Myth of Security at Canada's Airports, Standing Senate Committee on National Security and Defence*, 137th Parliament (2003), http://www.parl.gc.ca/Content/SEN/Committee/372/defe/rep/rep05jan03-e.htm, 69.

report for the European Parliament, Hobbing and Koslowski note that the U.S. is moving toward collecting and using biometric information, but, at the time the report was written, the TSA preferred that it happen at airline check-in as opposed to in the security line.[83]

To summarize: there are distinct levels of aviation that are generally treated differently from a security standpoint. Passenger screening is a visible and personal aspect of commercial airport security but practices vary widely, based on perceived utility and price. TCR has stated that its passengers will not undergo the type of intensive screening used at commercial aviation airports in the U.S. The type of passenger or baggage inspection that may or may not be employed by TCR is a decision that ultimately rests with the TSA, which has not said what it will require. It is probably a good indication of the type of screening to be used that airport-style screening is not currently used on ground transportation, such as buses or passenger trains. The Texas Legislature may wish to address the issue, given its history, or may wish to ensure that the issue can be addressed administratively.

## B. SECURITY MANAGEMENT

This high-speed rail proposal brings with it an array of homeland security concerns, and since it is a technologically-driven solution to a mass transportation problem, there are technology and human-related concerns at every turn. This section provides a literature review specifically regarding these concerns as raised by or applied to the TCR project. Technology is addressed through the subgenres of cybersecurity and energy/electrical, while human concerns addressed are insider threats and human error. Finally, supervisory control and data acquisition (SCADA) and train control is addressed in a later chapter.

[83] Peter Hobbing, and Rey Koslowski, "The Tools Called to Support the 'Delivery' of Freedom, Security and Justice: A Comparison of Border Security System in the EU and in the U.S. (Brussels: European Parliament, Directorate General for European Policies, 2009), http://www.europarl.europa.eu/RegData/etudes/note/join/2009/410681/IPOL-LIBE_NT%282009%29410681_EN.pdf, 36.

### 1. Cybersecurity

There is a wealth of literature in cybersecurity generally, cybersecurity for the private sector, and cybersecurity for critical infrastructure (primarily energy and electrical but also transportation).[84] Martin Rudner wrote:

> Cyber-attacks directed at Critical National Infrastructure constitute a significant, diverse, and rapidly escalating risk-element in the global threat environment. Critical infrastructures are susceptible to cyber-attacks precisely because of their high inherent value and intrinsic vulnerabilities, coupled with a significant potential to inflict widespread harm on targeted countries.[85]

The government has a duty to provide cyber protection for its activities and, by extension, the public sector. Many authors would extend that obligation to also cover the private sector. Rice, Miller, and Shenoi compare it to missile batteries placed around domestic population centers in the 1960s; they were to protect from incoming threats regardless of their targets. The authors also note that military cyber operations depend on other sectors for electricity and transportation, so they merit protection as well.[86] At a minimum, the military is red-teaming the use of cyber technology to derail American hazardous material trains.[87] Capra, writing from the U.S. Air Force (USAF) Counterproliferation Center, reports that "the Association of American Railroads testified before the U.S. Senate that the National Guard would be needed to secure critical assets during heightened states of alert." However, Capra points out that the National Guard would need to be operating under civilian authority to avoid violating the Posse Comitatus

---

[84] See, for example, Rita Tehan, *Cybersecurity: Authoritative Reports and Resources, by Topic* (Washington, DC: Congressional Research Service, 2014).

[85] Martin Rudner, "Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge," *International Journal of Intelligence and Counter Intelligence* 26, no. 3 (2013): 453–481.

[86] Mason Rice, Robert Miller, and Sujeet Shenoi, "May the U.S. Government Monitor Private Critical Infrastructure Assets to Combat Foreign Cyberspace Threats?" *International Journal of Critical Infrastructure Protection* 4, no. 1 (2011): 3–13.

[87] Anna Mulrine, "Cyber Security: The New Arms Race for a New Front Line," *Christian Science Monitor,* September 15, 2013, accessed December 27, 2014, http://www.csmonitor.com/USA/Military/2013/0915/Cyber-security-The-new-arms-race-for-a-new-front-line.

Act.[88] Bradbury provides legal support for the position that cyber-attacks are not a clear military action or events involving armed force,[89] and Rollins and Henning conclude that governmental mandates could be placed upon the private sector without invoking war powers.[90] Still, former Central Intelligence Agency (CIA) Director Hayden sounds skeptical when he writes about government's role in protecting critical infrastructure: "The statutory responsibility… falls to the Department of Homeland Security, but does it have the 'horses' to accomplish this? Do we await catastrophe before calling for DOD intervention, or do we move preemptively?"[91]

There is a distinction between the U.S. government's role in cybersecurity regarding the public and private sectors and its internal cyber processes, although they are related. The U.S. Department of Transportation (DOT) inspector general has cautioned, "DOT must also ensure the integrity of transaction data and reports that account for the billions of dollars used for highway reconstruction, high-speed rail development, and law enforcement grants."[92]

There is a limit to the role of government in cybersecurity. For instance, 70 percent of consumers responding to a ThreatTrack survey said government should not dictate to private companies how they should handle and store their private data, nor dictate which technologies businesses should use to secure their networks.[93] For even a limited role, Rice, Miller, and Shenoi place the responsibility at the federal level because of the multistate implications of possible scenarios but believe it should be a civilian

---

[88] Gregory S. Capra, "Protecting Critical Rail Infrastructure," *The Counterproliferation Papers, Future Warfare Series*, no. 38 (Maxwell Air Force Base, AL: U.S. Air Force Counterproliferation Center, Air University, 2006), 30.

[89] Steven G. Bradbury, *The Developing Legal Framework for Defensive and Offensive Cyber Operations* (Cambridge, MA: Harvard College, 2011).

[90] John Rollins, and Anna Henning, *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations* (Washington, DC: Congressional Research Service, 2009).

[91] Michael V. Hayden, "The Future of Things Cyber," *Strategic Studies Quarterly* (spring 2011): 1, http://www.au.af.mil/au/ssq/2011/spring/hayden.pdf.

[92] Calvin Scovel, *DOT Has Made Progress but Significant Weaknesses in its Information Security Remain* (Washington, DC: U.S. Department of Transportation, 2014).

[93] "Enterprise Executives and Consumers Lack Confidence about Cybersecurity," ThreatTrack Security, accessed December 27, 2014, http://www.threattracksecurity.com/resources/white-papers/executives-and-consumers-lack-confidence-in-cybersecurity.aspx.

authority, the Department of Homeland Security, in charge.[94] This is the case as a result of the Homeland Security Act of 2002, the *National Strategy to Secure Cyberspace*,[95] *Homeland Security Presidential Directive 7*, and *Presidential Policy Directive 21*, with the National Institute of Standards and Technology (U.S. Department of Commerce) leading the development of a critical infrastructure approach to cybersecurity under Executive Order 13636 (Improving Critical Infrastructure Cybersecurity).[96] Dinning of the U.S. DOT stresses collaboration and notes a variety of federal, nonprofit, and industry working groups in transportation cyber security,[97] and GAO's Wilshusen finds that between the public and private sectors, information is available but could be improved.[98] President Obama's *Comprehensive National Cybersecurity Initiative* of 2009, while focused on the federal enterprise, credits current cooperation between DHS and the private sector and calls for further definition of the federal role in extending cybersecurity into public and private sector critical infrastructure.[99]

### 2. Insider Threats/Human Error

Insider threats and human error are concerns in the context of technology. For instance, 67 percent of respondents to a 2014 Ponemon Institute survey of 599 global information technology (IT) and IT security executives said their companies had experienced at least one serious security compromise in the previous year; 24 percent of these respondents said the compromises were due to an insider attack or a negligent

---

[94] Rice, Miller, and Shenoi, "May the U.S. Government Monitor Private Critical Infrastructure," 3–13.

[95] David Powner, *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity* (Washington, DC: U.S. Government Accountability Office, 2005), http://www.gao.gov/assets/120/111987.pdf.

[96] National Institute of Standards and Technology, *Cybersecurity Framework Development Overview* (Washington, DC: National Institute of Standards and Technology, 2013).

[97] Michael Dinning, "Introduction to Cyber Security Issues for Transportation," webinar, John A. Volpe National Transportation Systems Center, December 7, 2011, https://www.pcb.its.dot.gov/t3/s111207_cybersecurity.asp.

[98] Gregory Wilshusen, *Critical Infrastructure Protection: Cybersecurity Guidance is Available, but More Can Be Done to Promote Its Use* (Washington, DC: Government Accountability Office, 2011), http://www.gao.gov/products/GAO-12-92.

[99] White House, *The Comprehensive National Cybersecurity Initiative* (Washington, DC: The White House, 2010).

privileged IT user.[100] DuBose, of Kroll Advisory Solutions, cites a number of studies with varying numbers but highlights the finding that insiders "are involved in more than two-thirds of all cyber cases involving theft of intellectual property."[101] Theft can take different forms, such as the case in which an employee of India's railway admitted that the IT office overseeing employees' financial information used a pirated version of Windows operating software—one with known vulnerabilities that could be exploited remotely.[102]

In addition to IT risks, there are other causes of accidents for rail trains. In one example from July 25, 2013, driver error is responsible for the crash of a Spanish high-speed train that killed at least 80 and injured another 130, as the technology on that track could not override the driver's control.[103] Electronic speed controls were subsequently installed.[104] In an American instance, a disgruntled freight railroad employee drove a locomotive without authorization onto the mainline and crashed it into another train.[105] To counter possibilities like this, Japanese railroad representatives respond that automated train controls will prevent signal violations and eliminate human error.[106]

The use of foreign technology raises questions about the extent of outsourcing to be employed with the Texas high-speed train project. Colwill's writing is representative

---

[100] Unisys Corporation, *Critical Infrastructure: Security Preparedness and Maturity* (Blue Bell, PA: Unisys Corporation, 2014).

[101] Michael DuBose, *The Insider Threat: Why Chinese Hacking May Be the Least of Corporate Worries* (New York: Kroll Advisory Solutions, 2013).

[102] Pulkit Vohra, "Cyber Security: Insider Threats—Government's Role in Protecting India's Critical Infrastructure Sectors" (master's thesis, University of Warwick, 2014).

[103] Laursen, "Spanish High-Speed Train Crash Offers Safety-System Lessons,"

[104] "Further Safety Measures Follow Santiago De Compostela Crash," *Railway Gazette*, August 5, 2013, accessed December 28, 2014, http://www.railwaygazette.com/news/policy/single-view/view/further-safety-measures-follow-santiago-crash.html.

[105] T. S. Jarmusz, "Disgruntled Employee Steals Train," *Gillette News Record*, October 12, 2014, accessed November 23, 2014, http://www.gillettenewsrecord.com/news/local/article_53a59dd3-6d5c-5353-a3f4-3e1d53c83398.html.

[106] Takao Nishiyama, *High-Speed Rail Operations in Japan* (New York: Japan Railways Group, 2010).

of the conventional wisdom that outsourcing increases the potential for misbehavior.[107] Other authors note that mitigating techniques are available.[108]

### 3. Conclusion

As a technology-based project, the proposed Texas high-speed train brings with it a range of concerns. Some, like various aspects of cybersecurity, are widely acknowledged and written about as they affect critical infrastructure in general, and a good amount of information is available in the more specific arena of transportation. Some are less frequently discussed in open sources, and these include proprietary information because of the privatized nature of the project and the use of foreign technology and processes.

To keep this writing to a manageable length, a number of issues are not included. For example, this thesis does not cover implications of electronic reservations and ticketing, which may open the system to outside connections and thus increase risk, nor does it cover potential concerns regarding the onboard provision of cellphone and Wi-Fi service, which may also increase potential entryways for malicious code or transmissions. Also outside of the scope of this thesis are explosive detection,[109] chemical threats similar to the Tokyo Sarin gas incident,[110] and deliberate non-interoperability with existing rail infrastructure[111] requiring a unique system of systems approach. Finally, also not included are right of way incursion detection[112] and fallout from the disruptive nature of the technology.

---

[107] Carl Colwill, "Human Factors in Information Security: The Insider Threat–Who can You Trust These Days?" *Information Security Technical Report* 14, no. 4 (2009): 186–196.

[108] Pravesh Gaonjur, and Chandradeo Bokhoree, *Risk of Insider Threats in Information Technology Outsourcing: Can Deceptive Techniques be Applied?* (Port Louis, Mauritius: University of Technology, 2006).

[109] Barkakati, and Maurer, *Technology Assessment: Explosives Detection*.

[110] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (Washington, DC: Government Printing Office, 2011).

[111] Benzion, "The Facts."

[112] Justin Yates, Rajan Batta, and Mark Karwan, "Optimal Placement of Sensors and Interception Resource Assessment for the Protection of Regional Infrastructure from Covert Attack," *Journal of Transportation Security* 4, no. 2 (2011): 145–169.

## C. SECURITY FORCE

### 1. Introduction

No governmental entity will own or operate this train. However, TCR has not publicly indicated how it will approach security, law enforcement, or other police activities related to the train project. Also, its public statements require some skepticism, as the developer's materials carry a disclaimer noting that plans are subject to change.[113]

The provision of security or policing is a key element of a public transportation system's protection. At a minimum, coordination between the police and the transportation security system greatly increases the likelihood of success for the system's security.[114] The following sections outline what is known about policing practices in Japan generally and as might be applied to the TCR system, discusses their potential applicability to the Texas project, and makes recommendations regarding optimal implementation.

### 2. Japan—The Country

The country of Japan is composed of multiple islands, and its total land mass covers about the same area as the state of California (see Figure 4). This small land mass supports a population of 127 million, of which 93 percent live in urban areas,[115] and land is at a premium. For administrative purposes, the country is divided into 47 prefectures (somewhat similar to states in the U.S.) with varying degrees of autonomy, size, and number of localities/municipalities contained therein.

---

[113] Benzion, "Texas Central Railway."

[114] Majid Sabzehparvar, and Seyyed Hossein Alavi, "The Role of Key Parameters in Public Transportation Security," *Journal of Transportation Security* 8, no. 1–2 (2015): 37–40.

[115] The source for this figure is the CIA World Factbook. It is significantly different from the 66 percent cited by Morag in *Comparative Homeland Security*. TheGlobalEconomy.Com, using World Bank and United Nations numbers, reports that urbanized population went from 64% in 1960 to 92% in 2013. The number is of interest in the context of this writing because of the comparison to Texas, which as of 2010, and, according to the U.S. Census Bureau, was 84.7 percent urbanized and the relevance of population urbanization and density to the operations of intercity high-speed passenger rail. "Japan Percent Urban Population," accessed December 6, 2015, http://www.theglobaleconomy.com/Japan/Percent_urban_population/;

U.S. Census Bureau, "2010 Census Urban and Rural Classification and Urban Area Criteria," last modified February 9, 2015, http://www.census.gov/geo/reference/ua/urban-rural-2010.html.

In 1854, Japan and the U.S. reached an agreement allowing American ships into Japanese ports for the first time.[116] Since that time, Japan and the United States have developed independently but participated in many of the same international organizations and enjoyed a close cultural and economic relationship, except for some unpleasantness in the 1940s. After 9/11, Japan participates in the war on terror and has good relationships with American intelligence.[117]

Figure 4. Size Comparison of Japan and the United States


Source: "Japan" [image], CIA World Factbook, accessed November 5, 2015, https://www.cia.gov/library/publications/the-world-factbook/graphics/area comparison/JA_area%202014.jpg.

116 "East and Southeast Asia: Japan," CIA World Factbook, last modified June 18, 2015, accessed June 20, 2015, https://www.cia.gov/library/publications/the-world-factbook/geos/ja.html.

117 Christopher Hughes, "Japan's Security Policy, the US-Japan Alliance, and the 'War on Terror': Incrementalism Confirmed or Radical Leap?" *Australian Journal of International Affairs* 58, no. 4 (2004): 427–445.

### 3. Japan's Approach to Policing

Japan maintains a sizeable police force and military. When necessary for securing public order, the military can be used in civil works. That ability became necessary in March of 2011, when a massive earthquake occurred in the Pacific close to the Tohoku region of northeast Japan.[118] The earthquake generated a tsunami of unprecedented height—16.7 meters, the height of a four story building—that devastated parts of Japan through immediate effect as well as caused the consequential breach of the Fukushima nuclear reactor.[119] Nobuo Mimura reports, "Over 24 thousand people were reported as dead or missing. The Ministry of Defense immediately dispatched assistance, including 110,000 active and reserve troops and 28,000 police to assist."[120]

The National Police Agency (NPA) is a single agency that serves all of Japan. The U.S. does not have a direct counterpart, although as part of its duties, the NPA is charged with gathering intelligence much like the Federal Bureau of Investigation (FBI). The NPA operates through seven regional police bureaus, the employees which include "high ranking officers in prefectural and local police forces."[121]

Prefectural headquarters supervise police stations. The largest police stations service Tokyo and Kita-Kyushu, and the smallest serves the remote fishing villages of Aomori Prefecture.[122] Police stations are organized into sections, including patrol, traffic, crime prevention, and criminal investigation. Under each station is a network of "kobans" (urban fixed police posts) and/or "chuzaisho" (rural residential posts).

Japan famously uses a community-based policing method. Urban policeman are known for their foot patrols and are addressed by the public as "Omawari-san"—Mr.

---

[118] Mimura et al., "Damage from the Great East Japan Earthquake and Tsunami," 803.

[119] Ichiro Fujisaki, "Japan's Recovery Six Months after the Earthquake, Tsunami and Nuclear Crisis," Brookings Institution, last modified September 9, 2011, accessed June 21, 2015, http://www.brookings.edu/events/2011/09/09-japan-recovery.

[120] James Jay Carafano, "One Year Later: Lessons from Recovery after the Great Eastern Japan Earthquake," *Heritage Foundation Special Report*, no. 108, 2012, http://www.heritage.org/research/reports/2012/04/one-year-later-lessons-from-recovery-after-the-great-eastern-japan-earthquake.

[121] Morag, *Comparative Homeland Security*, 3550–3557.

[122] David H. Bayley, *Forces of Order: Police Behavior in Japan and the United States* (Berkeley, CA: University of California Press, 1978), 20.

Walkabout. According to Bayley, patrolling does not lead to discovery of emergencies, reduce reaction time, or necessarily enhance availability. Foot patrols create authority through visibility and familiarity through face to face interaction. The involvement of Japanese policemen in day-to-day civic life goes beyond American crime prevention practices. Other activities include "lobbying for the construction of pedestrian overpasses, requesting that the sanitation department pick up trash and abandoned items, and asking business owners not to serve children during school hours."[123] Even so, patrolmen occupy the lowest rung of the police hierarchy.

### 4. Transportation in Japan

Japan has 175 airports, an advanced highway network, and a state of the art intra- and intercity rail-based transportation system. The subway network in Tokyo is the world's largest, with 30 separate train lines and 40 miles of tunnels. Moreover, Japanese passengers have had high-speed commercial train service as an option since October 1, 1964. Japan Railways operates eight bullet train routes covering about 1500 miles. The top speed presently permitted on the lines is 200 mph.[124]

### 5. Japan's Experience with Rail Security

In Japan, high-speed trains do not have a separate intelligence or security infrastructure; rather, these are integrated into the mass-transit structure with commuter and local trains.[125] Passengers boarding trains are not screened. Information about the true safety and security practices of Japanese trains is hard to come by, which may be a result of the privatized nature of the Japanese rail system. What stands out, however, is the sarin gas incident of 1995.

On the morning of March 20, 1995, hundreds of thousands of commuters boarded the Tokyo subways as usual, only this time five members of the Aum Shinrikyo cult

---

[123] Morag, *Comparative Homeland Security*, 3569–3570.

[124] Julian Ryal, "Bullet Train at 50: Rise and Fall of the World's Fastest Train," *The Telegraph*, last modified October 1, 2014, accessed June 21, 2015, http://www.telegraph.co.uk/news/worldnews/asia/japan/11133241/Bullet-train-at-50-rise-and-fall-of-the-worlds-fastest-train.html.

[125] Jenkins et al., *Formulating a Strategy for Securing High-Speed Rail in the United States*, 19.

joined the crowds on various subway lines. Four of the five carried two bags of sarin each while the fifth carried three bags. Sarin is an odorless, highly volatile synthetic nerve agent; exposure to it can lead to paralysis, respiratory failure, and death.[126] At 8 a.m., the cultists punctured the bags with umbrellas and fled the trains. The sarin leaked out of the bags and formed pools on the train floors. By day's end, a dozen people were dead. There were over 1400 seriously injured and 4,000 more who needed treatment for exposure to Sarin.[127]

Initial response was handled by the Tokyo Metropolitan Fire Department (TMFD). Of the 1,364 TMFD personnel who responded, 135 became victims themselves and required treatment; many had responded without personal protective equipment. The Tokyo Metropolitan Police Department (TMPD), which later took charge of the operation from the fire department under the supervision of the National Police Agency (NPA), mobilized 10,000 officers to increase security and provide crowd control.[128] However, even though the NPA knew that a hazardous material incident was occurring, trains continued to operate, although seven minutes behind schedule. The delay was because of the lag involved in one station realizing it had a problem when the train had already departed for the next, not due to the subway incident. The NPA eventually combined efforts with the military, borrowing hazmat suits and chemical warfare experts.

While the 1995 sarin gas incident is significant because of its nature and impact, for the purposes of this writing, it should be noted that it occurred in the subway, which while not a high-speed train, is part of the network that includes all commuter rail options.[129] Official Japanese materials regarding train safety typically omit this and other events or are worded to avoid mentioning them.

---

[126] "Facts about Sarin," Centers for Disease Control and Prevention, last modified May 20, 2013, accessed October 29, 2015, http://www.bt.cdc.gov/agent/sarin/basics/facts.asp.

[127] Testar, "What Tokyo Taught Us," 34–39.

[128] Ibid.

[129] Ibid.

### 6. Comparisons between Japan and the United States

The Posse Comitatus laws in the U.S. allow the use of military troops and equipment for only very limited civil purposes. While disaster response is allowed, arresting people is not. In addition, the military can and does perform other police functions jointly with police agencies, such as Joint Task Force 6's performance of reconnaissance, surveillance, weapons and communications training, and intelligence analysis at Fort Bliss, Texas in support of antidrug efforts.[130] This situation is unlikely to change given the history of the U.S. and the current political climate, particularly given the current public backlash against the use of surplus military equipment by civilian police forces.

In spite of this distinct difference in utilization of the military domestically, there are sufficient similarities between the United States and Japan as to make it possible to import security-related practices from one country to the other. David Bayley, in studying Japanese police institutions for possible lessons that could be applicable to the United States, wrote that Japan is comparable because it is "modern and affluent, congested and urbanized" and that modest differences in "technical capacity, educational levels, wealth, or dominant modes of production" do not impair the ability to make comparisons with the U.S.[131]

There are also differences that could mitigate these similarities. Cultural differences include approaches to marriage, parenting, employment, and religious practice. There are other differences, which, although seemingly minor, could have implications for the provision of security. For example, one study in 1994 found that, while face-to-face and telephone communication approaches are similar, American information technology workers prefer to communicate over distances using email while Japanese preferred fax.[132]

---

[130] Peter Andreas, and Richard Price, "From War Fighting to Crime Fighting: Transforming the American National Security State," *International Studies Review* 3, no. 3 (fall 2001): 31–52.

[131] Bayley, *Forces of Order: Police Behavior in Japan and the United States.*

[132] Detmar W. Straub, "The Effect of Culture on IT Diffusion: Email and FAX in Japan and the US," *Information Systems Research* 5, no. 1 (1994): 23–47.

In the public safety arena, both countries have had to address disaster preparation and response, have experienced terrorism (including in a rail transportation scenario), and have faced somewhat similar policing challenges. There are also some differences in the countries' approaches to a community policing model. First, there is a lack of agreement among American practitioners as to exactly what constitutes community policing.[133] Furthermore, there are discrepancies as to how similar policing methods are perceived in various American communities, such as in the African-American community, and there are aspects of community policing (e.g., visibility) that have unintended negative consequences (e.g., increased stop-and-frisks).[134] Other differences that could affect comparisons include that the Japanese do not treat of domestic violence crimes as a police matter.[135]

Bayley writes that the Japanese police system was deliberately developed as a hierarchical, top-down structure that gives the head of administration almost as much prestige as the chief of police. By contrast, American policing is fragmented. For instance, Texas alone has over 1900 non-federal law enforcement agencies. Two are the main statewide police agencies (Texas Department of Public Safety [DPS] and Texas Parks and Wildlife Department [TPWD]), and there are a broad range of state agencies with law enforcement powers (e.g., Texas Alcoholic Beverage Commission, Health and Human Services Commission). At the county level, there are elected sheriffs and constables, and at the municipal level police (some of whose chiefs are elected) and marshals. Furthermore, many special districts, such as school districts, transit authorities, public and private colleges and universities, and others, have law enforcement arms also. A number of these are transportation related. For example, the Dallas-Fort Worth International Airport is among the 10 largest nonfederal transportation-related agencies

[133] Gary Cordner, "Community Policing: Elements and Effects (1995)," in *The Oxford Handbook of Police and Policing*, ed. Reisig, Michael Dean, and Robert J. Kane (Oxford, UK: Oxford University Press, 2014), 148.

[134] Amy E. Lerman, and Vesla Weaver, "Staying Out of Sight? Concentrated Policing and Local Political Action," *The Annals of the American Academy of Political and Social Science* 651, no. 1 (2014): 202–219.

[135] Morag, *Comparative Homeland Security*.

for law enforcement in the country, and Harris County (Houston) and Dallas County transit authority police departments are in the top 15 on the same list.[136]

Regarding public confidence in policing, the Japanese people generally hold their police in high regard, which suggests broad acceptance of police processes; however, there is at least one quantitative study finding the opposite to be true. The study finds that the Japanese may have greater compliance with police but that does not necessarily translate into greater confidence.[137] The implication of this finding is that any application of Japanese practices to U.S. policing would need to be evaluated on the individual practice's merits as opposed to a more general assertion of superiority due to public acceptance.

### 7. Comparative Analysis of Approaches

Would the federalized nature of Japan's National Police Agency be beneficial if implemented in the U.S.? There already is something similar in effect in the area of railroad policing. Railroads in the U.S. are subject to the federal Transportation Security Administration, which can assert authority over public and private transportation systems. Like the NPA, the TSA cooperates with regional and local police agencies but can carry out its mission unilaterally. As a practical matter, in terms of law enforcement authority in relation to high-speed intercity passenger trains, the policing approaches are similar; however, most of the TSA's budget and focus is applied to aviation. While mass transit security was heightened after the London subway bombings in 2005, the sense of urgency has decreased, and there have been no significant permanent changes in the approach to mass transit security.[138]

Differences arise in regard to other police actions also. In Japan, there is a more hierarchical approach among the police agencies. In contrast, in the U.S., along the route

---

[136] Brian A. Reaves, "Census of State and Local Law Enforcement Agencies, 2008," last modified July 2011, accessed June 22, 2015, http://www.bjs.gov/index.cfm?ty=pbdetail&iid=2216.

[137] Liqun Cao, Steven Stack, and Yi Sun, "Public Attitudes toward the Police: A Comparative Study between Japan and America," *Journal of Criminal Justice* 26, no. 4 (1998): 279–289.

[138] Corona Brezina, *Public Security in an Age of Terrorism* (New York: The Rosen Publishing Group, 2009), 31–34.

of an intercity train there would be multiple police agencies (i.e., city, county, state, federal, special districts like transit authorities, possibly private railroad police) that should coordinate closely but may see themselves as competing with each other or asserting authority that may or may not exist. In the broader context, there is great hesitancy to creating a national police agency, which would have the potential for abuse as suggested by some authors, including Naomi Wolf.[139]

In Japan, police across the country wear identical uniforms and carry identical equipment in identical fashion: pistol on the right hip, handcuffs behind the left hip, nightstick by the left leg, and a length of light rope in a trouser pocket. In America, police agencies have distinct uniforms and insignia of office, and there may even be variations within a given police agency. There are advantages to uniformity of police who are not operating undercover in that they are easily recognized by the public across jurisdictions. This approach would be beneficial in the case of an intercity transportation mode that passes through a number of local jurisdictions as it would let the public know who has legal authority and can respond to incidents. In Texas, this would be obvious if the uniform is that of a state trooper but less obvious if the officer is from a local agency such as the transit districts likely to be found at the nodes of the train network, even though those officers may in fact have authority along the entire train network.

Bayley writes that there are significant differences between Japanese and American police in the areas of recruitment, training, pay, supervision, and accountability. Analysis of these differences is beyond the scope of this writing, but a cursory review does not indicate anything that would create a particular advantage or disadvantage regarding high-speed rail security. Bayley's discussion takes place mostly in the context of factors contributing to police misconduct. There are some notable differences between the police forces in the two countries, such as the Japanese police world is overwhelmingly male; this practice would not be allowed in the U.S. where police forces are largely integrated and military forces are becoming more so. The uniformity and similarity in training of Japanese police forces, resulting in a

[139] Naomi Wolf, *The End of America: Letter of Warning to a Young Patriot* (White River Junction, VT: Chelsea Green Publishing, 2007).

standardization of performance in a geographically dispersed, bureaucratic system lends itself to a certain sense of community. This is a challenge for the American model of multiple overlapping and occasionally competing agencies, which are mostly led by or responsible to elected officials, and therefore responsive to the community in a different way. Americans would be very suspicious of and opposed to law enforcement agents advocating for social or political change as part of their official duties (as opposed to police unions or association doing so on their own time).

The Japanese place a high priority on keeping the infrastructure functioning. For example, after the 2011 earthquake and tsunami, officials placed a high priority on cleaning up and restoring highways within two weeks. Railroads were back on normal schedules after about a month and a half.

The Japanese response to the sarin gas attack also included infrastructure-focused changes. Since the sarin gas attack, Japan has removed garbage cans from subway platforms, installed elevators as an additional escape route, established emergency headquarters facilities, and implemented an educational campaign similar to DHS's "see something, say something." In addition, surveillance cameras have been installed at stations and on trains.[140] In addition, under the auspices of the TMFD, hazmat training, and response guidelines have been widely promulgated. Direction from the highest levels of government has caused the various entities (e.g., police, fire, health, military) to cooperate and coordinate future efforts.

Due to the significant nature of the sarin gas attack, many of these improved terrorism prevention and response practices have already been adopted by agencies in the United States. However, I have been unable to identify anything in Japan that would be analogous to the U.S. Incident Management System, a superior method for coordinating agencies across jurisdictions.

Regarding operation of the train itself, TCR intends to use the system currently in place in Japan. These will include practices that are literally foreign to the U.S. because of the differences in system design. For example, in Japan the high-speed train tracks are

[140] Testar, "What Tokyo Taught Us," 34–39.

completely separated from freight tracks and road crossings. A special maintenance train is run before daily passenger service begins to confirm track and right-of-way integrity.[141] Adoption of these practices is a given and is not controversial.

### 8. Further Options

Texas law allows the state Department of Public Safety (DPS) to appoint peace officers employed by railroad companies through its director.[142] The law may need to be changed to increase the number of railroad peace officers allowed.

DPS is authorized to patrol toll roads,[143] including doing so through a contract.[144] TCR could contract with DPS for service.[145] Less directly, TCR could contract with off-duty DPS officers acting as private security guards in the same manner as any other business does. It is also possible to interpret Chapter 91 of the Texas Transportation Code as allowing TCR, through the Texas Department of Transportation, to have DPS provide law enforcement.[146]

### 9. Recommendation: Action Items

Concerns about security were heightened by the June 2015 suicide on board a Japanese HSR train and by the death of another passenger and Ayoub El Khazzani's August 2015 attempt to use multiple weapons on the Amsterdam-Paris train à grande vitesse (TGV, France's high-speed train). These concerns require active consideration in order to assure the public that the system is safe. It should be noted that ever since a man

---

[141] Kaiser, "High-Speed Rail Security Needs a Different Approach than Commuter Rail."

[142] "Texas Code of Criminal Procedure 2.121," Texas Constitutes and Statutes, accessed November 5, 2015, http://www.statutes.legis.state.tx.us/Docs/CR/htm/CR.2.htm#2.121.

[143] Vianna Davila, "High-Speed Toll Road Opening," *San Antonio Express-News*, October 24, 2012, accessed November 26, 2014, http://www.mysanantonio.com/news/local_news/article/High-speed-toll-road-opening-3974705.php.

[144] Transportation Code 366.182(c), "An authority may contract with any state or local governmental entity for the services of peace officers of that agency." "Transportation Code 366.182(c)," Texas Constitution and Statutes.

[145] See Siobhan O'Neil, "Relationship between the Private Sector and Fusion Centers Potential Causes for Concern and Realities," *Homeland Security Affairs*, Supplement no. 2 (2008).

[146] "Transportation Code Chapter 91. Rail Facilities," Texas Constitution and Statutes, accessed October 25, 2015, http://www.statutes.legis.state.tx.us/Docs/TN/htm/TN.91.htm.

jumped in front of a bullet train just after the line was opened in 1964, suicide by train has been a common occurrence in Japan. The incidents reached 800 successful such attempts per year by 2009,[147] compared to an annual average 45 suicides in the U.S. involving passenger rail.[148] These incidents draw public attention, heighten concern, and provide a legitimate area for policy consideration; however, the motivation and goal of these individuals generally is suicide, not martyrdom, multiple deaths, or terrorism. Suicide as a vector for or in combination with terrorism is certainly a possibility, along with shooters, car or truck bombs, biological or chemical weapons, or other mechanisms of attack. In 2009, there was a foiled suicide attack on a New York subway, and in 2008 an Al-Shabaab loyalist drove an explosive-laden truck into a government building in Somalis, becoming the first known instance of an American citizen conducting a terrorist suicide bombing.[149] However, as this writing is focused on vulnerabilities and the need for regulation as opposed to tactical threats, suicide bombers are not further addressed other than as part of generic threats.

To improve the provision of law enforcement and security regarding the private sector high-speed train system, the Texas Legislature should:

1. Consider whether the decision regarding how law enforcement is addressed for the TCR system occurs at the legislative level or at the discretion of the private sector corporation. In the absence of legislative action, the TCR will make those decisions in a fashion similar to other private sector intercity ground transportation providers. The direction chosen will affect how much of the Japanese security approach can be imported and where the gaps will occur.

2. Require verification that the planned design, construction, operation, and maintenance incorporate state-of-the-art security provisions no less than those currently practiced in Japan. The project is represented as using the system as it is in Japan, where proven security protocols are integrated into every aspect, including cyber systems, ticketing, and train control.

---

147 "Shinkansen Suicides," Socyberty, accessed November 14, 2015, http://socyberty.com/society/shinkansen-suicides/.

148 Jan L. Botha, Marissa K. Neighbour, and Satnam Kaur, *An Approach for Actions to Prevent Suicides on Commuter and Metro Rail Systems in the United States* (MTI Report 12–33), (San Jose, CA: Mineta Transportation Institute, 2014), 9.

149 Jerome P. Bjelopera, *American Jihadist Terrorism: Combating a Complex Threat* (Washington, DC: Congressional Research Service, 2013).

However, TCR has stated conditions may change, so it is necessary not to assume preparations in the area of security.

3. Task the Texas Department of Public Safety (DPS) with carrying out these actions in cooperation with other affected agencies and establish a Joint Legislative Oversight Committee to monitor implementation and receive regular reports regarding potential shortcomings. Since the Japanese top-down policing from the federal level is unlikely to be successful in the American context, the DPS is the logical point of coordination because as the statewide police agency whose jurisdiction includes rail and intelligence (although not exclusively) and whose force is regularly in every county, DPS is well positioned to provide enforcement or coordinate with the chosen enforcers and local agencies.

4. Should TCR determine to establish its own police force, require cooperation among that force and the various law enforcement and emergency response entities with jurisdiction over the train or its route. One lesson of the sarin gas incident is the importance of awareness, coordination, and practice among those who could be called upon in an emergency.

5. Require evidence that community sensitivities are taken into account in the establishment or importation of policing practices. If the community policing approach is adopted, the cultural diversity of the proposed train route necessitates consideration of customs and concerns.

6. If TCR employs its own police force, require its officers to wear distinctive uniforms and prohibit the implementation of practices such as political advocacy (which are beyond those currently authorized to American police agencies). Implementation of the Japanese practices regarding uniforms and political advocacy are significant departures from current practice and would require study and discussion before taking any further.

7. Study the potential for Japanese-style integration of high-speed rail trains into the commuter rail security system. Do this in recognition of the challenge presented by the interface between public and private systems and the physical separation of the high-speed train from grade crossings and freight rail lines as well as the multiple law enforcement jurisdictions involved. Finally, the potential benefits, as demonstrated by the safety record of the Japanese mass transit system, would require significant coordination at from all levels of government and the private sector along the TCR system's route.

These recommendations will enable the state to ensure its citizens' safety by allowing the private sector effort to make certain decisions regarding its approach to law enforcement,

employing methods that have proven effective in daily practice in Japan, limiting Japanese practices where they are incompatible with American systems and culture, and employing lessons learned in Japanese police practice as appropriate.

## D. INFORMATION SHARING

TCR faces many challenges in providing security for its HSR project. One challenge is how the company can best protect its investment and passengers through the efficient gathering and sharing of information about possible threats (intel). TCR will certainly be acquiring intel in the course of its business operations. So will public and private law enforcement entities, transit providers, and other critical infrastructure entities in the region. Terrorism prevention will depend on how well intel is collected, compared, analyzed, and resolved.

### 1. Importance of Intel to High-Speed Rail

Having good intel is critical.[150] Of 15 planned attacks against public transportation between 1997 and 2010, 11 were uncovered by intel[151] as was a 2013 Canadian passenger train plot.[152] In addition, intel has been critical in stopping high-speed rail terrorist plots.[153] DHS believes that long-distance, passenger train systems should have "access to robust information-sharing networks that include relevant intel and threat analysis and real-time incident reporting."[154] When the DHS inspector general criticized Amtrak for not focusing more on hardening rail stations, TSA responded that

---

[150] James Jay Carafano, Steve Bucci and Jessica Zuckerman, "Fifty Terror Plots Foiled since 9/11: The Homegrown Threat and the Long War on Terrorism," *Backgrounder 2682*, April 25, 2012, http://www.heritage.org/research/reports/2012/04/fifty-terror-plots-foiled-since-9-11-the-homegrown-threat-and-the-long-war-on-terrorism.

[151] Jenkins, and Trella, "Carnage Interrupted."

[152] Bob Paulson, "RCMP Arrests Two Individuals for Terrorism-Related Charges," Royal Canadian Mounted Police, April 22, 2013, accessed November 23, 2014, http://www.rcmp-grc.gc.ca/news-nouvelles/2013/04-22-ns-sn-eng.htm.

[153] Jenkins et al., *Formulating a Strategy for Securing High-Speed Rail in the United States*

[154] Michael Chertoff, *FY 2006 Infrastructure Protection Program: Intercity Passenger Rail Security, Program Guidelines and Application Kit* (Washington, DC: U.S. Department of Homeland Security, Office of Grants and Training, 2005).

Amtrak's operational activities, including intel, are "just as important" in critical infrastructure protection.[155]

Nextgov cites former officials as finding shortcomings in the way intel is currently developed and employed for the protection of critical infrastructure. According to Sternstein:

> While government and critical industry sectors have made strides in sharing threat intelligence, less attention has been paid to translating those analyses into usable information for the people in the trenches, who are running the subways, highways and other transit systems, some former federal officials say.[156]

The State of Texas will not own or operate this train or its stations, so its responsibilities are limited, but regardless of the adequacy of private sector efforts, government has a compelling role regarding all critical infrastructure protection, through collaboration, regulation, or both.[157]

### 2. The Japanese Approach

In Japan, high-speed rail trains do not have a separate intel or security infrastructure; rather, they are integrated into the mass-transit structure with commuter and local trains.[158] Passengers boarding trains are not screened, but surveillance cameras were installed at stations and on trains after the 1995 sarin gas attacks.[159]

After 9/11, Japan participated in the war on terror and is seen to have good relationships with American intelligence.[160] Additionally, the CEO of TCR is reportedly

---

[155] Anne L. Richards, *DHS Grants Used for Mitigating Risks to Amtrak Rail Stations* (Washington, DC: Department of Homeland Security, Office of Inspector General, 2011).

[156] Aliya Sternstein, "Hackers Manipulated Railway Computers, TSA Memo Says," *Government Executive*, January 23, 2012, http://www.nextgov.com/cybersecurity/2012/01/hackers-manipulated-railway-computers-tsa-memo-says/50498.

[157] Rudy Darken, and Ted G. Lewis, "Potholes and Detours in the Road to Critical Infrastructure Protection Policy," *Homeland Security Affairs* 1, no. 2 (2005): 8, https://www.hsaj.org/articles/177.

[158] Jenkins et al., *Formulating a Strategy for Securing High-Speed Rail in the United States*, 19.

[159] Ibid.

[160] Hughes, "Japan's Security Policy."

a former CIA officer posted to Tokyo[161] and later the Bush administration's top defense policymaker for Asia[162] who can be expected to have good ties in both the American and Japanese intel communities.

### 3. Options for Efficient Intel

Fusion centers enable relationships necessary for intel.[163] At least two of Texas's seven fusion centers are in the train's service area (Dallas and Houston) and one has statewide jurisdiction, the Texas Joint Crime Information Center (JCIC) in Austin).[164] Centers will need to collaborate, not compete. TCR has several options with regard to how it provides security that will affect how efficiently the railroad can share intel. These are listed in the sections that follow.

#### *a. Option 1: Standard Intercity Passenger Security*

TSA has broader reporting requirements than states do.[165] The TSA by federal rule receives intel and significant concerns about security from the rail security coordinator (RSC) for each passenger railroad.[166] . However, TSA may withhold from state and local governments an RSC's identity and contact information.[167] Private intercity bus lines coordinate with local police and are eligible for DHS bus security

---

161 Crawford, "The Big Texas Plan to Copy Japan's High-Speed Rail Success."

162 "US Defense Policymaker Richard Lawless Resigns," *Taipei Times*, April 6, 2007.

163 Michael T. McCaul, and Peter King, *Majority Staff Report on the National Network of Fusion Centers*, United States House of Representatives Committee on Homeland Security, accessed November 24, 2014, https://homeland.house.gov/files/documents/CHS%20SLFC%20Report%202013%20FINAL.pdf, 47.

164 "Fusion Center Locations and Contact Information," U.S. Department of Homeland Security, accessed November 24, 2014, http://www.dhs.gov/fusion-center-locations-and-contact-information.

165 Ibid.

166 73 Fed. Reg. 72130 (2008).

167 Ibid.

grants[168] (there are similar grants for rail[169] but Amtrak is the only eligible entity[170]). TCR could approach security in the same manner as intercity buses. TSA's security can range from random checks to airline-style checkpoints, but the president of TCR has rejected "TSA-type security."[171] While public transit agencies can employ their own peace officers,[172] TCR does not fit the current legal definition of public transit agency. TCR might be able to rely on existing transit police at terminals but these officers would be limited to their home agencies' geographic jurisdiction without a change in law and their participation in fusion centers is unknown as of this writing.

#### *b. Option 2: Private Rail Police*

As noted earlier, Texas law allows the state Department of Public Safety (DPS) to appoint peace officers employed by railroad companies through its director.[173] TCR would need to establish relationships and communication mechanisms, which under this scenario could occur through fusion centers' private sector outreach. The law may need to be changed to increase the number of railroad peace officers allowed. Railroads are represented on DHS critical infrastructure boards, and the Joint Crime Information Center (JCIC) in Austin, as the official Texas state fusion center, has a critical infrastructure protection component that emphasizes involvement of the private sector.[174]

---

168 "Catalog of Federal Domestic Assistance: Intercity Bus Security Grants," General Services Administration, accessed November 26, 2013, https://www.cfda.gov/index?s=program&mode=form&tab=core&id=e231a6d500f4c652fb4ba6cc3e325298.

169 "Catalog of Federal Domestic Assistance: Rail and Transit Security Grant Program," accessed November 26, 2014. https://www.cfda.gov/index?s=program&mode=form&tab=core&id=e231a6d500f4c652fb4ba6cc3e325298.

170 "Funding Opportunity Announcement: FY 2014 Intercity Passenger Rail (IPR)—Amtrak," accessed November 26, 2014, http://www.tsa.gov/sites/default/files/publications/pdf/grants/tsgp/FY_2014_IPR_FOA.pdf.

171 Judge Robert Eckels speaking on a panel at the Texas Tribune Festival. *Is High-Speed Rail Really Happening?* Transportation Panel, 2014, Texas Tribune Festival, September 13, 2014, https://soundcloud.com/texas-tribune-festival/sets/the-texas-tribune-festival-7.

172 For example, Transportation Code 451.108 authorizes Houston Metropolitan Transportation Authority to employ peace officers. "Transportation Code Chapter 451. Metropolitan Rapid Transit Authorities," accessed October 25, 2015, http://www.statutes.legis.state.tx.us/Docs/TN/htm/TN.451.htm#451.108.

173 "Texas Code of Criminal Procedure 2.121," Texas Constitutes and Statutes.

174 "TxDPS—November 10th, 2014 Texas Joint Crime Information Center."

### *c. Option 3: Texas Department of Public Safety*

As noted earlier, DPS is authorized to patrol toll roads,[175] including doing so through a contract.[176] TCR could contract with DPS for service with a direct connection to the state fusion center to avoid concerns about private sector involvement in fusion centers[177]—regardless of their validity.[178] Less directly, TCR could contract with off-duty DPS officers acting as private security guards in the same manner as any other business does; this would have the benefit of informal personal networks. It is also possible to interpret Chapter 91 of the Texas Transportation Code as allowing TCR, through the Texas Department of Transportation, to have DPS provide law enforcement.[179]

### 4. Conclusion

Potential threats to HSR require efficient intel and careful consideration of TCR's approach to law enforcement. TCR's setup and management provide a ready level of interaction with intel, but since DPS is responsible for the Texas Fusion Center,[180] the most efficient course would be for TCR to participate with DPS in its various intel programs for the private sector.

## E. PROTECTIVE MEASURES ASSESSMENT

The train is a potential target for terrorists. As a detailed study of hard (infrastructure) and soft (human or other non-infrastructure) protective measures is beyond the scope of this writing, this section examines whether and how the company can anticipate and prepare for a singular, well known aspect of terrorism: the

175 Davila, "High-Speed Toll Road Opening."

176 Transportation Code 366.182(c), "An authority may contract with any state or local governmental entity for the services of peace officers of that agency." "Transportation Code 366.182(c)," Texas Constitution and Statutes.

177 See German, and Stanley, *What's Wrong with Fusion Centers?*

178 See O'Neil, "Relationship between the Private Sector and Fusion Center."

179 "Transportation Code Chapter 91. Rail Facilities," Texas Constitution and Statutes.

180 "Government Code, Title 4, Subtitle B, Chapter 421, Subchapter E," Texas Constitution and Statutes, accessed October 25, 2015, http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.421.htm#421.081.

psychological effects of terrorism upon employees, customers, emergency responders, and residents along the train's path. It looks at pre-event, event, and post-event considerations.

### 1. Potential Impact of an Act of Terrorism—Financial

In addition to the immediate physical injuries, fatalities, or property damage that occur in an act of terrorism, there are likely to be other negative effects, including financial impacts. While the various studies can occasionally be contradictory in aspects, they are generally in agreement the negative effects of a terrorism incident continue for some duration after the incident.

After the events of September 11, 2001, there was a significant decline in the number of people choosing to fly. According to one set of researchers, the result was both "a negative transitory shock of over 30% and an ongoing negative demand shock amounting to roughly 7.4% of pre-September 11th demand."[181] These effects went through at least 2003 and are unlikely to be attributable to outside factors, such as the general economy, the Iraq war, or the SARS outbreak.[182] The implementation of baggage screening has led to a five to eight percent reduction in people flying.[183] Several airlines approached bankruptcy and were only saved by federal intervention.[184] Blalock, Kadiyali, and Simon estimate "the substitution of driving for flying by those seeking to avoid security inconvenience alone likely led to over 100 road fatalities."[185]

The airlines of the planes that crashed in 9/11 were sued by families and businesses, and these lawsuits resulted in further financial losses. Cantor Fitzgerald, a

[181] Harumi Ito, and Darin Lee, "Assessing the Impact of the September 11 Terrorist Attacks on U.S. Airline Demand," *Journal of Economics and Business* 57, no. 1 (2005): 75–95.

[182] Ibid.

[183] Garrick Blalock, Vrinda Kadiyali, and Daniel H. Simon, "The Impact of Post-9/11 Airport Security Measures on the Demand for Air Travel," *Journal of Law and Economics* 50, no. 4 (2007): 731–755.

[184] Scott S. Blunk, David E. Clark and James M. McGibany, "Evaluating the Long-Run Impacts of the 9/11 Terrorist Attacks on U.S. Domestic Airline Travel," *Applied Economics* 38, no. 4 (2006): 363–370.

[185] Blalock, Kadiyali, and Simon, "The Impact of Post-9/11 Airport Security Measures," 731–755.

New York brokerage firm, settled its lawsuit with American Airlines for $135 million.[186] Additionally, United Airlines settled a lawsuit with at least one family for an undisclosed sum.[187] From a standpoint solely of financial considerations, a corporation, at a minimum, would have a duty to its shareholders to act upon the possibility of terrorist acts by taking steps to prevent such acts.

### 2. Potential Impact of an Act of Terrorism—Behavioral

The purpose of terrorism is to instill dread, reduce confidence in government structures, and create a "fearful state of mind in an audience far wider than the immediate victims." It is "political warfare on a psychological field of battle."[188]

In natural disasters, unintentional man-made disasters, and incidents of terrorism, society experiences a disruption of normalcy and safety, both in the immediate area and in a wider context.[189] However, incidents of terrorism have some qualities that distinguish them from natural disasters and unintentional man-made disasters. The potential impact of terrorism is greater and more severe than other disasters because of these qualities and their effects on "distress responses, behavioral change, and psychiatric illness."[190] For example, terroristic events are committed on purpose with the desired outcomes of injuries, damage, attention, and fear to achieve political ends. These events are largely unpredictable, although the list of potential targets can be narrowed through an examination of significance, vulnerability, and threat. Another quality of terrorism that sets it apart from other disasters is that prevention may be possible.

---

186 Julia Talianova, "Cantor Fitzgerald, American Airlines Settle 9/11 Lawsuit," *CNN*, December 17, 2013, http://www.cnn.com/2013/12/17/us/new-york-cantor-fitzgerald-american-settlement/index.html.

187 Benjamin Weiser, "Last 9/11 Wrongful-Death Suit is Settled," *The New York Times*, September 19, 2011.

188 Lisa Butler, Leslie Morland, and Gregory Leskin, "Psychological Resilience in the Face of Terrorism," in *Psychology of Terrorism*, ed. Bruce Bongar et al. (400–417), (New York: Oxford University Press, 2007).

189 Ibid., 406.

190 Adrienne Stith Butler, Allison M. Panzer, and Lewis R. Goldfrank, eds. *Preparing for the Psychological Consequences of Terrorism: A Public Health Strategy*. Washington, DC: National Academies Press, 2003. http://www.nap.edu/catalog/10717.html, 45.

Like financial changes, behavioral changes from terrorism may also be long lasting. According to David Myers, there are four key drivers of fear: what we are historically predisposed to fear, what we cannot control, what is immediate, and what is most readily available in memory, especially if tied to a horrific image or images.[191] A quality of terrorism is that it excels in at least three of these areas.

As a result of the Tokyo sarin gas attack of 1995, a dozen people died, over 1400 were seriously injured and 4,000 more needed treatment for chemical exposure. According to records, "sixty percent of the victims also had to be treated for post-traumatic stress disorder."[192] Two years after the event, survivors continued to report "symptoms such as fear of subways (32 percent), sleep disturbances (29 percent), flashbacks (16 percent), and irritability (10 percent)."[193] Victims presented somatic and psychological symptoms five years after the event.[194]

Furthermore, psychological effects have been known to contribute to or be significant risk factors for physical ailments, including chronic diseases and the relationship between stress and heart disease. Trauma can "affect everyday behavior, including social and individual behaviors related to half of all causes of U.S. morbidity and mortality."[195] Thus, an act of terrorism could have negative financial, physical, and behavioral effects.

### 3. Potential Victims

Taylor identified six categories of potential victims of terrorist attacks:

> Those who are adversely affected at the epicenter of a disaster, their families and close friends, the emergency workers and those whose jobs

---

[191] David G. Myers, "Do We Fear the Right Things," *APS Observer* 14, no. 3 (2001): 31 accessed December 6, 2015, http://www.psychologicalscience.org/index.php/publications/observer/2001/december-01/do-we-fear-the-right-things.html.

[192] Testar, "What Tokyo Taught Us," 34–39.

[193] Panzer, Butler, and Goldfrank, *Preparing for the Psychological Consequences of Terrorism* 61.

[194] Ibid., 49

[195] Susan E. Brandon, and Andrew P. Silke, "Near and Long-Term Psychological Effects of Exposure to Terrorist Attacks," in *Psychology of Terrorism*, ed. Bruce Bongar et al. (175–193), (New York: Oxford University Press, 2007).

> oblige them to become directly involved in the rescue and recovery operations, the grieving community that identifies with those who are suffering, the psychologically troubled whose reactions are exacerbated, along with troublemakers who are inclined to exploit the situation and use it to their own advantage.[196]

Taylor also includes various other people who are adversely affected.[197]

Should a train be the subject of a terrorist attack, it can be expected there would be psychological impacts for anyone involved in or anyone who perceives they could have been involved in the incident. This list includes physically affected victims, people in close proximity but not directly affected, first responders, employees of the company, and people living or working along the route of the train. It could also include a wide array of others: people indirectly or remotely affected, such as those seeing pictures of the event through broadcast or social media; those whose livelihoods are impacted by economic effects of the incident; and those with some affinity to the incident through knowing, being related to a victim, or by perceiving the attack as being on a broader social identity group, such as Texans. These groups will experience vulnerability and the potential for negative psychological outcomes. The may be substantial variation in the kind of vulnerability, and the presence and extent of vulnerability may not be readily apparent.[198] Furthermore, the effects will vary given proximity to an incident and how prepared an individual is to experience such an incident.

Generally, people who experience traumatic stress react by having negative thoughts, feelings, and behaviors. For instance, they may experiences common psychological effects, including difficulty concentrating and remembering as well as having recurring images and dreams of the disaster. Additionally, common feelings people may have include fear and anxiety, sound and smell triggers, irritability, hopelessness, and depression. Furthermore, common behaviors of people may include

---

196 Anthony J. W. Taylor, "Defusing the Terrorism of Terror," in *Psychology of Terrorism*, ed. Bruce Bongar et al. (New York: Oxford University Press, 2007), 384, Kindle edition.

197 Ibid.

198 Panzer, Butler, and Goldfrank, *Preparing for the Psychological Consequences of Terrorism*, 54.

being overprotective, hyper-alert and startling easily, and crying for no apparent reason.[199]

In the Tokyo sarin gas incident, people who were not in the area of the incident and had no rational reason to believe they had been victims of this or any related attack sought treatment.[200] About three quarters of those who sought medical care showed no effects of exposure to sarin.[201] Fear and anxiety led these "worried well" to consume health resources that were otherwise needed and engaged. Their arrival at hospitals actually exposed them to hazards they would not otherwise have experienced because the time lag in diagnosing sarin led to a secondary exposure in the hospital setting as sarin gas was released from the skin, clothing, and hair of the victims awaiting treatment. Also, due to inadequate diagnosis and lack of proper personal protective equipment, at least 12 doctors showed symptoms of secondary exposure.[202]

Effects on emergency providers, such as law enforcement, first responders, pre-hospital and hospital, and fire, are pronounced and extend beyond those directly impacted to include those indirectly involved. Impacts are felt differently by different special groups.[203] Special groups could be defined by age (e.g., children), culture, ethnicity, socioeconomic status, gender, and possibly history of psychiatric illness.[204] Some researchers include in the emergency responder category those utility workers involved in immediate service restoration, such as electricity and water.[205]

Incidents on trains and in train stations specifically are challenging because they are confined spaces with large numbers of people and few limitations on presence or travel. The "flight" option of the fight-or-flight choice is constrained—by confined spaces, by the number of other people, or both. Additionally, train movement and related

---

[199] Jacobs quoted in Panzer, Butler, and Goldfrank, *Preparing for the Psychological Consequences of Terrorism*, 42.

[200] Panzer, Butler, and Goldfrank, *Preparing for the Psychological Consequences of Terrorism*, 53.

[201] Ibid., 61.

[202] Testar, "What Tokyo Taught Us," 34–39.

[203] Panzer, Butler, and Goldfrank, *Preparing for the Psychological Consequences of Terrorism*, 46.

[204] Ibid., 43.

[205] Ibid., 25.

activity, such as route maintenance, happen on regular, known schedules. As seen in Japan, disruptions would affect not just one train and its occupants but also subsequent trains and passengers, feeders systems, such as parking and transit, first responders, local health networks, and corporate personnel.

For the government, responsibility to provide support to disaster victims and their families, including related preparatory measures, falls initially to the National Transportation Safety Board (NTSB). The NTSB Transportation Disaster Assistance Division coordinates all levels of government and non-governmental groups as well as liaising with the carrier in addressing the issues of those affected.[206]

### 4. Recommendations

While the ability to predict the exact effects of terroristic acts has proven elusive, there is general agreement that there are behavioral and psychological impacts of terrorism in addition to the physical damage. A goal of minimizing these impacts would suggest that emergency, medical, public health, and psychological management steps should be taken preparing for an event, in responding to an event, and in recovering from an event.[207]

First, just as planners are budgeting for and planning the logistics of traveler safety through such efforts as train and station design, purchase of onboard first aid equipment, and arrangements with first responders along the route, they should also include psychological and mental health in those preparations. The psychological consequences of an act of terrorism are likely to affect economic resiliency as well as emotional well-being beyond those physically involved.[208]

The corporation should actively anticipate and plan for mental needs by determining what role it will take and what role the public sector, private sector (e.g., private medical facilities), and nonprofit sectors are willing to perform, then assessing the

---

[206] "Transportation Disaster Assistance (TDA)," National Transportation Safety Board, accessed November 5, 2015, http://www.ntsb.gov/tda/Pages/default.aspx.

[207] Butler, Panzer, Goldfrank, eds., *Preparing for the Psychological Consequences of Terrorism.*

[208] Ibid., 107.

relative abilities and any gaps in the desired level of service. First responders in particular should be trained in mental health as specifically applied in disasters, including the notable features resulting from terrorism. Community services at train stations and along the route, such as public and private healthcare providers and facilities and even treatment centers for substance abuse, should be identified and mapped along with their normal and surge capacities, which could then be compared with train passenger loads to reveal potential service shortages that should be addressed. This approach will be more effective if communities are invited and actively participate in the pre-event planning process.

The corporation should also plan for accurate and timely communication with the public and authorities during and after events. Resulting benefits should include a reduction in instances of people whose health is not affected but they think it might be—the so-called worried well—attempting to access the system and overwhelming its capabilities. In addition, the corporation should consider an appropriate and effective pre-event risk communication strategy. This strategy could include instructions designed to limit the likelihood of a terrorist attack (e.g., see something say something) and to anticipate and limit confusion and uncertainty during and after the event (e.g., active shooter scenario behavior, first aid information, how to exit, where to gather, and how to locate loved ones in an emergency).

To address employee wellness, the corporation should consider incorporating mental health protocols into business continuity plans. These protocols might include planning for off-site family support centers, an employee locator system, and alternate power systems for during and post-incident activity.[209]

### 5. Conclusion

The potential for serious psychological impacts from a terrorist attack on the proposed Texas Central Railway high-speed train merits appropriate planning and preparation. Certain steps can be taken to reduce the impact on the corporation, its shareholders, customers, and the public.

[209] Ibid., 112.

## F. DEPENDENCIES

Passenger transportation systems depend on other sectors for necessary inputs that they cannot or will not provide themselves. The DHS National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis has identified sectors on which mass transit particularly relies. According to DHS:

> Mass transit systems are dependent on these Sectors [energy, emergency services, communications, information technology, and financial services] to maintain daily operations; provide power, oil and gas; data communications, including the exchange of industrial control system data that integrates different functions (e.g., operations, location tracking, emergency alarms, fire detection, gas monitoring); emergency response and recovery; and daily financial transactions.[210]

### 1. SCADA/Train Control

With the Stuxnet incident having received wide media coverage and industry concern[211] and at least one additional incident causing significant destruction at an industrial facility in Germany,[212] there is extensive responsive literature addressing "supervisory control and data acquisition" (SCADA, defined as "a generic name for a computerized system that is capable of gathering and processing data and applying operational controls to geographically dispersed assets over long distances").[213] SCADA is generally recognized as presenting cyber vulnerabilities; however, there is disagreement regarding the extent of the vulnerability in the rail transportation world. A report in the *New York Times* stated that then-Secretary of Defense Leon Panetta told an audience, "An aggressor nation or extremist group could use these kinds of cyber tools to gain control of critical switches…. They could derail passenger trains, or even more

---

[210] U.S. Department of Homeland Security, *Sector Risk Snapshots* (Washington, DC: U.S. Department of Homeland Security, Office of Cyber and Infrastructure Analysis, 2014), http://nacchopreparedness.org/wp-content/uploads/2014/05/OCIA-Sector-Risk-Snapshots.pdf, 43. See Mass Transit Mode pull out, page 2.

[211] Paul K. Kerr, John Rollins, and Catherine A. Theohary, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability* (Washington, DC: Congressional Research Service, 2010).

[212] Kim Zetter, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," *Wired*, last modified January 8, 2015, accessed November 14, 2015, http://www.wired.com/2015/01/german-steel-mill-hack-destruction/.

[213] Robin Williams, "SCADA," s.v., *Cyber Glossary*, National Initiative for Cybersecurity Careers and Studies, accessed December 26, 2014, http://niccs.us-cert.gov/glossary.

dangerous, derail passenger trains loaded with lethal chemicals."[214] It should be noted that the existence of "passenger trains loaded with lethal chemicals" would be hyperbole at best and alarming otherwise, but in this instance, it appears to be a reporting error by the *New York Times* that was repeated by many other outlets, including UPI.[215] A review of a video of the event[216] and the official transcript prepared by the Department of Defense[217] reveals that the reference to trains loaded with lethal chemicals meant freight trains, not passenger trains.

Mass transit (passenger rail) and freight rail both use SCADA systems to control such things as track direction, railroad signals, switches, and automated control processes.[218] Unlike freight rail's flexible and difficult to predict schedule, long-distance passenger trains run on published schedules with little tolerance for variation. For instance, the average delay time for a Shinkansen train in Japan is a minute or less, and the turnaround time for the Shinkansen at Tokyo Station, which handles 300 trains per day with four tracks and two platforms, is 12 minutes.[219] The Japanese Shinkansen uses an extensive network of automated train and traffic control systems.[220] Figure 5 shows the Integrated Intelligent Transport Management System Computerized Safety, Maintenance, and Operation Systems (COSMOS of Shinkansen).

---

[214] Elisabeth Bumiller, and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on US," *The New York Times*, October 11, 2012, sec. World.

[215] "Panetta: 'Cyber-Pearl Harbor' Possible," *UPI*, October 12, 2012, accessed December 28, 2014, http://www.upi.com/Top_News/US/2012/10/12/Panetta-Cyber-Pearl-Harbor-possible/UPI-15331350047855/.

[216] Leon Panetta, "Secretary Leon Panetta on Cybersecurity, Speaking to the Business Executives for National Security at the Intrepid Sea, Air and Space Museum in New York City," *C-SPAN*, October 11, 2012, accessed December 28, 2014, http://www.c-span.org/video/?308750-1/secretary-leon-panetta-cybersecurity. At the 18:30 mark.

[217] Leon Panetta, "Transcript: Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City," U.S. Department of Defense, accessed December 28, 2014, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

[218] Abby Doll et al., *Critical Infrastructure and Cyber Security* (College Station, TX: George Bush School of Government and Public Service, Texas A&M University, 2011).

[219] Nishiyama, *High-Speed Rail Operations in Japan*.

[220] Tamura, *An Overview of Japan's High Speed Rail: Shinkansen*.

Figure 5. The Integrated Intelligent Transport Management System COSMOS


Source: Nishiyama, High-Speed Rail Operations in Japan.

In America, in August of 2011, the hacker collective Anonymous breached cybersecurity at Bay Area Rapid Transit (BART) of San Francisco and released personal information regarding over one hundred BART police officers.[221] Security officers at Class I railroads are quick to acknowledge this breach and point out that it involved business records, not any operational or control circuits.[222]

This incident notwithstanding, the potential for operational disruption does exist. Such a thing happened in Poland in 2008. A Polish teenager altered a television remote control and was able to redirect trams in Lodz as if it were "a giant train set," derailing four trams and injuring 12 people.[223] According to former TSA Administrator Kip Hawley, "They are in better communication with trains than airlines are with their

[221] Rachel King, "Anonymous Hacks BART Police website; Publishes Officers' Info," ZDNet, August 17, 2011, accessed December 26, 2014, http://www.zdnet.com/article/anonymous-hacks-bart-police-website-publishes-officers-info/#!

[222] Sneider, "Railroad Communication and Signal Article."

[223] Graeme Baker, "Schoolboy Hacks into City's Tram System," *The Telegraph*, January 11, 2008, accessed December 1, 2014, http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html.

airplanes."[224] Hawley was speaking about freight railroads, but his point is applicable to the technology in question; railroads are in constant communication with their trains and even have control over them. Knowledge of cyber threats pertaining to railway networks is hampered though, according to Wijesekera of George Mason University's Center for Infrastructure Protection, because existing American railway networks "do not have mechanisms for the comprehensive, secure, centralized collection of forensic data."[225]

Brito and Watkins note that Clarke and Knake, in the 2010 best seller *Cyber War*, describe the derailment of trains as a possible outcome of a cyber war scenario. However, Brito and Watkins believe any such threat is overstated, as the Clarke-Knake scenario is based on "distributed denial of service" attacks (DDOS). In addition, Brito and Watkins are skeptical that a DDOS attack would be sufficient to derail a train.[226] Dumont disagrees, however, suggesting attacks would go beyond DDOS to include reconfiguring instructions, data, or code.[227] Aliya Sternstein, writing in NextGov and citing a TSA memo, wrote that foreign hackers were able to control signals and disrupt train traffic on a freight railroad for two days in 2011. However, the industry adamantly disputes the accuracy of the TSA memo, holding that the incident described did not occur, and DHS appears to be distancing itself from the memo.[228] However, Robert Turk of the Idaho National Laboratory wrote that CSX Transportation has acknowledged a worm that in 2003 infected its communication system, "affecting the dispatching and signaling systems such that all passenger and freight traffic, including morning commuter traffic in the Washington, D.C., area, had to be stopped for about 12 hours."[229]

---

[224] Kip Hawley, *Steel Wheel Security*, YouTube Video, February 8, 2013, http://youtu.be/B2Rhn6iLAk0. At the 3:20 mark.

[225] Duminda Wijesekera, "Critical Rail Infrastructure Protection Research at George Mason University," *The Critical Infrastructure Report* 7, no. 8 (2009).

[226] Jerry Brito, and Tate Watkins, "Loving the Cyber Bomb-the Dangers of Threat Inflation in Cybersecurity Policy" (working paper, Arlington, VA: Mercatus Center, George Mason University, 2011), http://mercatus.org/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy.

[227] Dennis Dumont, "Cyber Security Concerns of Supervisory Control and Data Acquisition (SCADA) Systems" in *IEEE International Conference on Technologies for Homeland Security (HST)*, 2010, DOI 10.1109/THS.2010.5654964.

[228] Sternstein, "Hackers Manipulated Railway Computers, TSA Memo Says."

[229] Robert J. Turk, *Cyber Incidents Involving Control Systems* (Idaho Falls, ID: Idaho National Engineering and Environmental Laboratory, 2005).

Will there be real-time communication with or control from Japan? This may improve efficiency but create vulnerability. Paul Rosenzweig notes the important connection between the cyber world and the physical, citing that a 2006 earthquake off the coast of Taiwan cut six of seven undersea telecommunications cables, disrupting Internet traffic to Japan and several other countries.[230]

### 2. Energy and Electrical

TCR's proposal involves an all-electrically powered system. There are parallels between the train project and the electrical grid itself. Production, transmission, and sale of electricity are primarily private sector activities. The electric power system has historically been both a war and peacetime target, with numerous instances of attack by state and non-state actors around the world. The electric grid serves a public purpose and its protection is in the public's interest.

One major difference between the electrical system and the high-speed train is the effect of a successful terrorist attack. Immediate injuries and fatalities are more likely on the train or at any of the train's key points (e.g., stations, trainset, right-of-way) whereas a grid failure could indirectly lead to injuries or fatalities through loss of critical health support systems, traffic control devices, and perhaps prolonged loss of power to refrigeration, air conditioning, and heating units.[231] Still, as this is not a new threat, hospitals and other sensitive energy users have access to backup generators, distributed generation, and other methods that can stave off damage to human life in all but the most widespread and prolonged disruptions.[232]

Another major difference is that there is little uniformity or standardization among the various pieces of the grid. A wide variety of suppliers and manufacturers are

---

[230] Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World* (Santa Barbara, CA: Praeger, 2013), 290.

[231] A drug cartel's attack on electrical systems in Mexico resulted in five deaths, but this appears to be an exception. See Madeline Vale, *Securing the U.S. Electrical Grid* (Washington, DC: Center for the Study of the Presidency and Congress, 2014).

[232] Lester B. Lave et al., "Increasing the Security and Reliability of the U.S. Electricity System," in *The Economic Impacts of Terrorist Attacks, Cheltenham, UK, and Northampton, Mass*, ed. Harry W. Richardson, Peter Gordon, James E. Moore, III, and Edgar Elgar (57–69), (Cheltenham: Edward Elgar Publishing, Inc., 2005), http://ise.usc.edu/assets/007/64864.pdf.

available that can supply the necessary equipment[233] except possibly high voltage transformers, which are not manufactured in this country and can take many months to manufacture.[234] This heterogeneity creates complexity and multiple potential points of failure within the system, but it also increases the possibility that, in the event of failure, a substitute can be found or quickly implemented. By contrast, the proposed high-speed train is a homogenous system that has been tested and refined in daily use; however, major components, such as railcars, do not currently have suppliers in the U.S. In addition, contingency plans would need to take into consideration the relative merits of maintaining inventories of parts versus the time required to receive shipments from Japan.

Various technological concerns regarding electrical power are inherent in the project, as the train is powered by electrical power supplied by overhead catenary cable.[235] Electricity brings with it high-tech issues such as SCADA,[236] vulnerabilities including cyberattack, physical attack, directed energy weapons, geomagnetically induced currents, and severe weather.[237] Electricity also brings lower-tech issues such as in the Arkansas incident where a determined vandal pulled powerlines down over some tracks far enough that a train snagged them.[238] This is a particularly noteworthy item as the proposed project seeks to share right-of-way with existing roads and utilities.[239] Light rail systems and subways typically do not have backup electrical power systems beyond

---

[233] Madeline Vale, *Securing the U.S. Electrical Grid* (Washington, DC: Center for the Study of the Presidency and Congress, 2014).

[234] Tom Glass, "Op-Ed: Texas must Protect our Grid against Attack—the Feds Won't," Breitbart Texas, last modified April 19, 2015, accessed November 15, 2015, http://www.breitbart.com/texas/2015/04/19/op-ed-texas-must-protect-our-grid-against-attack-the-feds-wont/.

[235] Benzion, "Texas Central Railway."

[236] U.S. Department of Homeland Security, *Sector Risk Snapshots*.

[237] Vale, *Securing the U.S. Electrical Grid*.

[238] Will Stephenson, "The Story of Jason Woodring, the Arkansas Power Grid Vandal," *Arkansas Times*, June 12, 2014, accessed December 28, 2014, http://www.arktimes.com/arkansas/the-story-of-jason-woodring-the-arkansas-power-grid-vandal/Content?oid=3334926.

[239] Stephen Green, "Company Planning High-Speed Rail Project," *The Huntsville Item*, October 1, 2014, http://www.itemonline.com/news/article_3c34e4b0-4907-11e4-b2dd-131f33bc7d85.html.

emergency lighting.[240] The proposed train, its control systems, and the grid are also potentially vulnerable to natural or man-made electromagnetic pulse.[241] Finally, there are likely to be implications for energy use and air quality as passenger rail systems around the world move to generated electricity as a power source,[242] but that discussion is beyond the scope of this writing.

### 3. Positive Train Control

Federal law requires intercity passenger trains to use positive train control—a designation for a system of computer processors communicating over wired or wireless networks to control train speed and movements.[243] There are a variety of architectures or approaches that could be used to implement positive train control, which is intended to reduce or eliminate collisions. However, due to a variety of factors and complications, most American freight and commuter railroads have not fully implemented positive train control. Estimates for full implementation are no earlier than 2017 and possibly even 2020 or later.[244]

Japanese trains currently use a positive train control-like process.[245] TCR has not said how its process will comply or vary from legally required processes in the U.S. Positive train control does increase safety, but it is at the possible expense of cybersecurity due to an increased reliance on radio frequencies and computer software controlled systems. Railroad computer systems have proven to be vulnerable to cyber

---

[240] M. Granger Morgan, *Terrorism and the Electric Power Delivery System* (Washington, DC: National Academies Press, 2012).

[241] *U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Electromagnetic Pulse (EMP): Threat to Critical Infrastructure*, 113th Cong. (2014), https://homeland.house.gov/hearing/subcommittee-hearing-electromagnetic-pulse-emp-threat-critical-infrastructure/.

[242] Vaibhav Chaturvedi and Son H. Kim, "Long Term Energy and Emission Implications of a Global Shift to Electricity-Based Public Rail Transportation System," *Energy Policy* 81 (2015): 176–185.

[243] Robert Scieszinski, "Positive Train Control (PTC) Overview (Railroad Safety)," Federal Railroad Administration, accessed November 23, 2014, http://www.fra.dot.gov/Page/P0621.

[244] Susan Fleming, "Positive Train Control: Additional Authorities could Benefit Implementation," U.S. General Accounting Office, last modified September 16, 2013, accessed November 15, 2015, http://www.gao.gov/products/GAO-13-720.

[245] Tamura, *An Overview of Japan's High Speed Rail: Shinkansen*.

threats. In one incident from 2011, hackers accessed Bay Area Rapid Transit computer systems and stole customer and employee information.[246] In another, the TSA at least initially ascribed a 2011 passenger train delay to a cyber-attack, possibly a foreign one.[247]

[246] Julie Sneider, "Railroad Communication and Signal Article - Railroads Gear Up to Protect Computers from Hackers," *Progressive Railroading Magazine*, September 2012, accessed November 23, 2014, http://www.progressiverailroading.com/c_s/article/Railroads-gear-up-to-protect-computers-from-hackers--32354.

[247] Sternstein, "Hackers Manipulated Railway Computers, TSA Memo Says."

# IV. PROBABILITY AND FAULT TREE ANALYSIS

## A. INTRODUCTION

Previous chapters have addressed the potential for acts of terrorism and the possible outcomes or consequences of such acts. The worst possible outcomes would include deaths and physical destruction that would have a negative effect on public opinion, disrupt train operation, create expense on the parts of responding entities, and have a negative economic effect on the corporation and related activities. This chapter addresses the question of the potential (or likelihood or probability) of such an act happening. This is the third piece of the three pieces that typically are combined to represent risk.[248]

## B. QUALITATIVE VERSUS QUANTITATIVE APPROACHES

Measuring risk involves identifying an event type and determining the frequency of that event, the severity of the outcome, which can be measured using fatalities, injuries, physical damage, business lost due to shutdowns or delays, and other impacts, and then attempting to project that into the future. Understanding the probability of an event is a necessary component of risk analysis because, combined with action and consequence, it allows a comparison of threats and vulnerabilities and, therefore, a format for decision making regarding the allocation of scarce resources. For the HSR system, this could mean choosing among various security options, such as fortifying stations, right-of-way surveillance, intrusion detection systems, and cyber protection. It could also mean balancing security with measures that increase passenger through-put, and ideally, it facilitates such federal activities as the award of security grants.[249] However, even that use should be tempered with some subjective or political factors that take into account factors such as the value to a terrorist organization of a successful strike. If one only compared transit to car travel on the basis of death rates, one would focus safety efforts

[248] Jonas Erikkson, and Anna-Karin Juhl, *Guide to Risk and Vulnerability Analyses* (Karlstad: Swedish Civil Contingencies Agency, 2012), 46.

[249] David R. Peterman, *Passenger Rail Security: Overview of Issues* (Washington, DC: Congressional Research Service, 2005), 7.

on automobile travel. According to Todd Litman, using U.S. death rate by mode statistics, "Even including terrorist attacks and other crimes against transit passengers, transit is far safer than private vehicle travel."[250]

At its most basic level, estimating probabilities requires the identification of necessary or contributing factors and evaluating their place in a qualitative analysis. A more advanced approach is to identify historical, cultural, and other markers that can be used to develop a quantitative analysis. In theory, these analyses can become quite granular, comparing a variety of types of attacks (e.g., long guns, explosives, cyber, chemicals) at a variety of locations (e.g., outside stations, inside stations, under bridges) at different times of the week or day (e.g., first train out, rush hour).

The more quantitative the approach, the greater the ability to compare subtly nuanced and finely detailed scenarios. However, the user of these methods should be aware of the potential shortcomings because they also could have consequences. The first and most obvious shortcoming is that they all involve predicting the future, a dicey proposition under the best of circumstances. Our ability to do so as relates to terrorism has had some successes but some notably spectacular failures.

Not only do these analyses require predicting the future, but quantitative approaches that use historical data mean predicting the future based on past terrorist incidents. Yet, one hallmark of terrorism is that while certain markers do tend to be constant (e.g., pre-operational surveillance, selection of soft targets) others change, seem to vacillate, or evolve (e.g., law enforcement/military or civilians as targets, methods, and tempo of communication, recruitment). Also, the more granular the analysis, the fewer historical incidents are available, and therefore, the margin of error is likely to increase. As well, there may be many options as to which measures are chosen for comparison (e.g., public mass transit, intercity trains, intercity high-speed trains; U.S., countries with HSR, worldwide; total track miles, passenger train miles, passenger miles).

[250] Todd Litman, "Terrorism, Transit and Public Safety: Evaluating the Risks," *Journal of Public Transit* 8, no. 4 (2005): 36.

A study attempting to compare the safety of rural and urban areas using car crashes would find quantitatively more crashes in cities than in the countryside and conclude the countryside is safer. Yet, as Jeff Speck wrote in a Twitter post on November 19, 2015, "FYI, if this map showed collisions per capita, it would be the opposite. Cities much safer than suburbs or country."[251] Furthermore, as the Swedish Civil Contingencies Agency simply stated, "The method for probability assessment chosen affects the use of the analysis results."[252] This topic falls under a developing field of research called "probabilistic terrorism risk assessment,"[253] which is seeing a lively internal debate regarding various methods and their effects on outcomes. For example, writing about nuclear power plant vulnerability, Peplow, Sulfredge, Sanders, and Morris offer modified approaches, stating:

> The results of vulnerability analysis are greatly influenced by the computational approaches used. Standard approximations used in fault-tree analysis are not applicable for attacks, where high component failure probabilities are expected…. Different blast modeling approaches can also affect the end results. Modeling the structural details of facility buildings and the geometric layout of components within the buildings is required to yield meaningful results.[254]

There will also be conditions, externalities, and items difficult to quantify that could change the outcomes. To the extent that the train as proposed is a closed system, in that it does not interact with freight tracks or rely on outside systems beyond those noted in the chart of dependencies, the potential for disruption is reduced. To the extent that redundancies and fail safes are built into the system, as is likely given what can be learned from public information about the Japanese experience, the possibility of normal accidents or disruptions leading to catastrophic failures is reduced.

---

[251] "Twitter Post, 8:29 PM November 19, 2015," last modified November 19, 2015, accessed November 21, 2015, https://twitter.com/JeffSpeckAICP/status/667530285844680704.

[252] Erikkson, and Juhl, *Guide to Risk and Vulnerability Analyses*, 45.

[253] Mark G. Stewart et al., "Probabilistic Terrorism Risk Assessment and Risk Acceptability for Infrastructure Protection," *Australian Journal of Structural Engineering* 13, no. 1 (2012): 2.

[254] Douglas E. Peplow et al., "Calculating Nuclear Power Plant Vulnerability using Integrated Geometry and Event/Fault-Tree Models," *Nuclear Science and Engineering* 146, no. 1 (2004): 71.

## C. POTENTIAL DATA SOURCES

The Mineta Transportation Institute maintains the Database of Terrorist and Serious Criminal Attacks Against Public Surface Transportation, that contains historical information on several thousand incidents, broken down using over 50 different types of targets and plots.[255] However, this database is proprietary and not available to the general public for queries, so findings using its data cannot be corroborated without special clearance.

The University of Maryland and the National Consortium for the Study of Terrorism and Responses to Terrorism (START) maintain the Global Terrorism Database,[256] which can be queried by the public online at http://www.start.umd.edu/gtd/. The Global Terrorism Database catalogs over 6000 transportation incidents as opposed to the 3000 incidents in the Mineta database.[257] Strandberg used the Global Terrorism Database to identify 3,955 terrorist attacks against public transportation, of which 1,122 involve rail.[258] However, the Global Terrorism Database does not break down the target or attack details to the extent Mineta does.

The Federal Railroad Administration's Office of Safety Analysis provides a publicly accessible database of freight and passenger railroad operations. The database includes incident and casualty information and can be viewed, queried, and downloaded online at http://safetydata.fra.dot.gov/OfficeofSafety/default.aspx.

## D. FAULT TREES

For complex systems, fault trees are a visual diagramming method of identifying points in the system that are most prone to failure or more critical due to their role in a potential failure. Fault trees can be devised using the system pieces identified through the

---

[255] "Factsheet-MTI Database," HS University, last modified September 2013, accessed November 22, 2015, http://www.hsuniversityprograms.org/default/assets/File/Factsheet-MTI database-FINAL-as of Sept2013.pdf.

[256] Gary LaFree, and Laura Dugan, "Introducing the Global Terrorism Database," *Terrorism and Political Violence* 19, no. 2 (2007): 181–204.

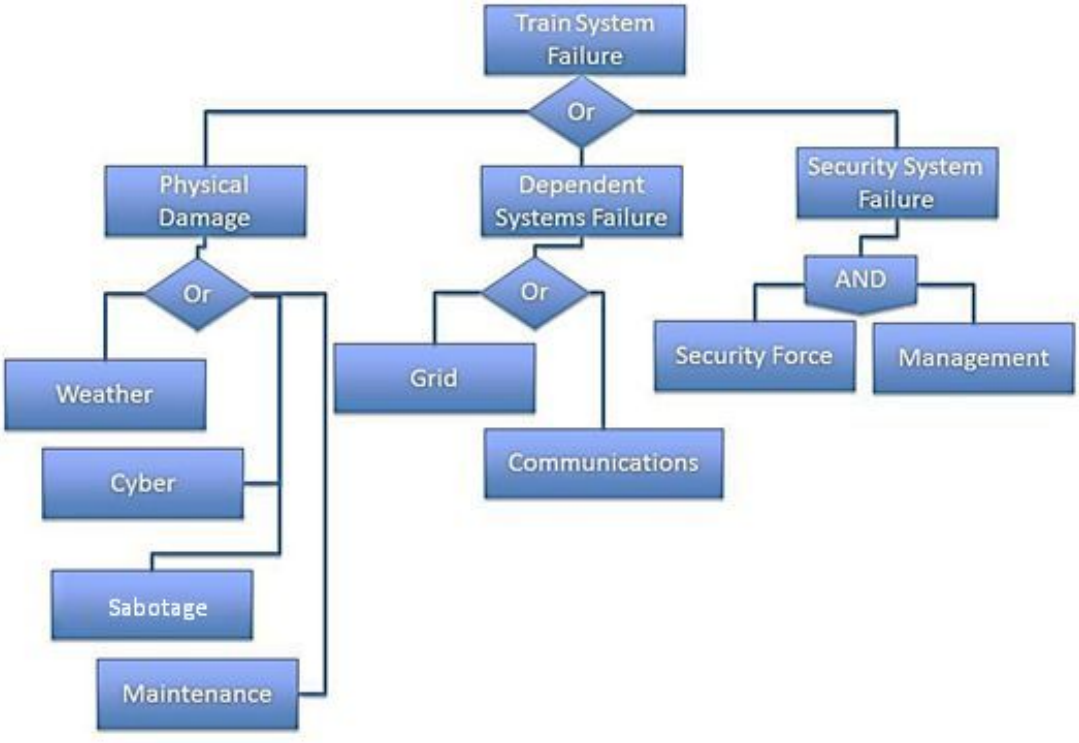
[257] "Factsheet-MTI Database," HS University.

[258] Veronica Strandberg, "Rail Bound Traffic: A Prime Target for Contemporary Terrorist Attacks?" *Journal of Transportation Security* 6, no. 3 (2013): 274.

major components approach, and each component can be further broken down into subcomponents and sub-subcomponents to provide a greater ability to analyze potential areas of vulnerability.

The worst possible outcome for this project would be a terrorist act and a catastrophic failure of systems involving deaths and physical destruction that would have a negative effect on public opinion, disrupt train operation, create expense on the parts of responding entities, and have a negative economic effect on the corporation and related activities. A fault tree analysis allows a structured consideration of the potential sub-system failures that could factor into a catastrophic system failure. Figure 6 illustrates a proposed set of interconnections among subsystems for this analysis.

Figure 6. HSR Fault Tree

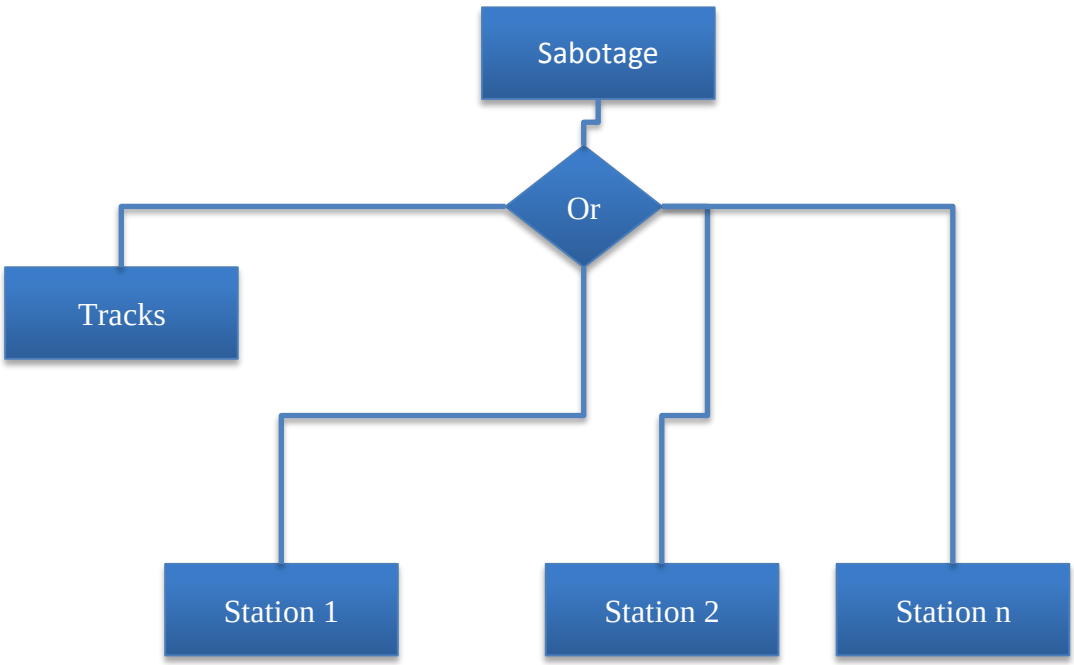



In the proposed approach, a catastrophic train system failure could result from three key sources: physical damage to the system, failures of interconnected systems that

the train system depends on, or failures in the security system. These sources appear as the first level below the OR gate in Figure 6. In this example, actions sufficient to create catastrophic failure through physical damage could occur in the areas of weather, cyber/ information technology, sabotage, or maintenance. Actions sufficient to create catastrophic failure through failure of dependencies could occur in the energy/electrical or communications areas. For a securities system failure sufficient to bring the entire system down, actions in either the security force or security management areas by themselves would not be sufficient, but failures in both areas must occur, hence the AND gate at the second level in Figure 6. Each of these system threats could be further evaluated, creating additional branches in the fault tree. The proposed tree is not meant to be exhaustive but to illustrate the approach.

Further analysis can be conducted within the sub-areas. For example, Figure 7 shows a subset of items that could be vulnerable to sabotage.

Figure 7. Fault Tree for Sabotage




In Figure 7, sufficient damage could occur at track locations or at any station to bring about overall system failure. As the number of track miles or stations increase, the

possible points of failure increase, and therefore the probability of failure, all other things being equal, would increase.

A useful exercise at this point might be to calculate an exceedance probability. Exceedance probability uses historical data to calculate the odds of a certain occurrence happening. Occurrences of concern in this example happen either along the track or at a station. According to published sources, the TCR project will initially have one station in Houston,[259] at least one in Dallas, and one near Shiro to serve Bryan/College Station and Huntsville[260] for a total of at least three.

The formula for determining the probability of successful sabotage then depends on the probability of track failure multiplied by the probabilities of failure of any given station:

$$\left(1 - P_f\right) = (1 - P_{f-track})(1 - P_{f-station1})(1 - P_{f-station2})...(1 - P_{f-station-n})$$

where $\boldsymbol{P_f}$ is the overall probability of successful sabotage (failure probability), $\boldsymbol{P_{f\text{-}track}}$ is the probability of track failure, and $\boldsymbol{P_{f\text{-}station}}$ is the probability of failure of any given station.

Developing an exceedance probability for track failure requires calculating terrorist incidents per mile of track to calculate an incident per mile measure. That number could further be refined using consequence data (fatalities/injuries). However, track miles affected by terrorist incidents around the world are difficult to acquire, and the one successful terrorist incident on American rail, given the miles that Amtrak uses and the years of service, will on its face provide a very high probability of exceedance. Over time, as data becomes available, such an analysis might prove useful. Regardless of the availability of these data, however, it is clear that the failure probability of the system increases with the length of track and the number of stations.

---

259 "The Private Texas High-Speed Rail Line Won't Stop in Downtown Houston," CityLab, last modified November 19, accessed November 22, 2015, http://www.citylab.com/commute/2015/11/amid-great-progress-texas-high-speed-rail-takes-a-big-step-back/416733/?utm_source=nl__link5_111915.

260 AECOM, *Dallas to Houston High-Speed Rail Project Alignment Alternatives Analysis Report* (Washington, DC: Federal Railroad Administration, 2015), 4.

THIS PAGE INTENTIONALLY LEFT BLANK

# V. OPTIONS ANALYSIS

## A. INTRODUCTION

This chapter provides a quantitative approach to analyzing the macro-level policy options. The State of Texas is faced with two possible approaches to this new HSR activity:

1. Texas requires homeland security standards for the proposed high-speed train (action) and
2. Texas does not require homeland security standards for the proposed high-speed train (status quo).

The possible outcomes are:

1. There is no attack (including the possibilities that an attack was prevented, or thwarted before it reached the operational stage);
2. An attack occurred but was unsuccessful (another way of saying this would be that an attack occurred that we were prepared for); and
3. An attack occurred that was successful/an attack occurred for which we were not prepared.

Looking at the issue from the perspective of the State of Texas, it would find more utility in not adding requirements because this approach would minimize any additional effort and cost. However, the probability of attacks, and those attacks being successful, increase if Texas does not act (this assumes that under the status quo, Texas already has requirements that are compatible with but supplemental to federal requirements, are in addition to any security plan initially implemented independently by the railroad company, and are effective). Under either option, the utility drops precipitously if an attack is successful. On the one hand, all things being equal, one might expect the utility of a successful attack to be more under the status quo option than under the action option because less money and effort have been expended to achieve the same outcome; however, there is a political factor involved. Should an attack be successful, a government that has not directed action toward the issue will be perceived more negatively than a government that has taken steps but not done enough.

This chapter provides a quantitative comparison of the status quo and active approach options using the utility tree analysis as outlined by Morgan D. Jones.[261] Conducting a quantitative comparison and analysis under this method involves two variables and a product. A variable is assigned to provide a measure of the utility of a given outcome for each approach. Another variable is assigned as an estimate of how likely that given outcome might be for each approach. The two variables are multiplied together to get the product—the expected value—which takes the utility of an outcome and tempers or conditions it based on the likelihood of its occurrence. After the assignment of utility values U, the estimate of likelihood of outcome xP, and the calculation of the expected value (EV=U*xP). The results are then ranked to reveal the most desirable choice. For this exercise, I have assigned a fairly high likelihood of attempted terrorist attack under the status quo option, 80 percent, based on a subjective evaluation of the quantitative and qualitative analysis of various conditions described elsewhere in this writing. Table 2 contains the quantitative calculations of a utility matrix for state regulation of high-speed rail security.

Table 2. Utility Matrix for State Regulation of High-Speed Rail Security

| Perspective: State of Texas | | Outcome | | | Total EV | Rank |
|---|---|---|---|---|---|---|
| | | No Attack/ Attack Prevented/ Attack Thwarted | Unsuccessful Attack (Attack for which we are prepared) | Successful Attack (Attack for which we are not prepared) | | |
| Option | Texas Acts | U 90<br>xP .6<br>EV 54 | U 80<br>xP .3<br>EV 24 | U 10<br>xP .1<br>EV 1 | 79 | 1 |
| | Status Quo | U 100<br>xP .2<br>EV 20 | U 90<br>xP .4<br>EV 45.6 | U 0<br>xP .4<br>EV 0 | 65.6 | 2 |

[261] Morgan D. Jones, *The Thinker's Toolkit: Fourteen Powerful Techniques for Problem Solving* (New York: Three Rivers Press, 1998), 252.

## B. ANALYSIS

The expected values came out lower and closer than I had anticipated. I may have been a little harsh on the combined federal and corporate effort in the absence of state regulation, assigning an 80 percent chance that an attack is attempted without state action. However, even if I double that to a 40 percent probability of no attack under the status quo and reduce the probability of successful attack to .3, the ranking stays the same. The ranking would change if I reduced the probability of an unsuccessful attack when unregulated to .3, but that would then be the same probability as an unsuccessful attack when regulated, which I do not believe is supportable.

If I were going to add other perspectives, I might consider the issue from the angle of the railroad company, the TSA, the property owners along the route, and the passengers. Generally, the railroad company would find more utility in less regulation. I do not have enough information to speculate as to the federal government's preference or if they would have one. While Texans are known generally for preferring limited regulation, property owners along the route would probably perceive benefits to additional homeland security and prefer state action but would also want the additional requirements paid for by the corporation as opposed to tax dollars. Passengers, in my estimation, would be neutral to favorable toward more regulation as long as regulations were perceived to provide more security and were unobtrusive; however, regulations that impede the process or are perceived as heavy handed (e.g., TSA-style passenger screening) would have less utility. As my writing is intended to inform state policymakers, I weigh heavily the state's perspective.

THIS PAGE INTENTIONALLY LEFT BLANK

# VI. CONCLUSION

There is a history of terrorist actions against passenger trains and stations, including on HSRs. Even so, this writing is the first in its specific application to the TCR project. A review of the various major components and selected subcomponents shows vulnerabilities and the potential for current or future threats in these areas. A fault tree analysis suggests that a failure of any of four of the six major components could have catastrophic results. An analysis of options shows that under certain assumptions the state should act, either by directly requiring certain homeland security standards or by assigning state agencies with responsibilities regarding security for the TCR project proposed to connect Dallas and Houston, Texas.

The proposed system is similar to an existing system in Japan, which has experienced fatalities and injuries during operation. In addition, several high-speed passenger systems around the world have experienced terrorist attacks, as has the Japanese rail system, although not its high-speed rail system directly. Security for the proposed system can be evaluated using a framework developed by the Argonne National Laboratory and combining what we know about the proposed system with what we have learned from experience with railroads, passenger transportation, electric and cyber systems, and terrorist incidents.

The State of Texas should require homeland security standards for high-speed rail. These standards would provide a baseline set of requirements for projects of this nature and could include how law enforcement is achieved, how the project interacts with the intelligence community, considerations regarding cyber security, passenger privacy, vulnerability and threat assessment, and participation in planning committees. This topic will be of interest to an audience of policymakers, homeland security practitioners, and possibly even the project developers. It provides some flexibility so that if this project should cease, the research would lay the groundwork for a paradigm applicable to future projects.

Texas may wish to take a formal position regarding passenger and baggage screening, and it may also desire to set certain standards or requirements regarding cybersecurity as well as the collection and control of transaction data, including personally identifiable information. An overarching question for consideration is whether the legislature sets requirements, authorizes an agency like the DPS to set requirements, or allows the new project to go forward within the framework of existing laws. Given the unique and precedent setting nature of the project, the legislature should be proactive in creating specific requirements or expectations and in ensuring that state enforcement agencies have sufficient authority to ensure the provision of public safety for a private sector transportation project. These requirements may include a legal ability to acquire and enforce representations made regarding the system's security provisions.

The state may wish to mandate how this enterprise will share or participate in sharing intel with law enforcement agencies, and it may specifically assign responsibility to the DPS for enforcement and oversight, including ensuring that the chosen method of policing and sharing intel complies with law and is effective. Other responsibilities having to do with emergency response may also be assigned, possibly to other state units like the Department of State Health Services, which may address mental health plans, for example, as appropriate. Legislative leaders may wish to designate an oversight committee or committees to monitor the project and ensure that public concerns are addressed appropriately.

# LIST OF REFERENCES


Andreas, Peter, and Richard Price. "From War Fighting to Crime Fighting: Transforming the American National Security State." *International Studies Review* 3, no. 3 (fall 2001): 31–52.

Baker, Graeme. "Schoolboy Hacks into City's Tram System." *The Telegraph*, January 11, 2008. Accessed December 1, 2014. http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html.

Barron, Inaki. "50 Years of High Speed Rail." *UIC e-News*, no. 418. October 7, 2014. International Union of Railways. Accessed December 7, 2014. http://uic.org/com/uic-e-news/418/.

Batheja, Aman, and Stephen J. Smith. "The Bullet Train that Could Change Everything." *The Texas Tribune*, August 18, 2014.

Bayley, David H. *Forces of Order: Police Behavior in Japan and the United States*. Berkeley, CA: University of California Press, 1978.

Benzion, David. "Texas Central Railway." Texas Central Railway. Accessed September 21, 2014. http://texascentral.com/.

Bjelopera, Jerome P. *American Jihadist Terrorism: Combating a Complex Threat*. Washington, DC: Congressional Research Service, 2013.

Blalock, Garrick, Vrinda Kadiyali, and Daniel H. Simon. "The Impact of Post-9/11 Airport Security Measures on the Demand for Air Travel." *Journal of Law and Economics* 50, no. 4 (2007): 731–755.

Blunk, Scott S., David E. Clark and James M. McGibany. "Evaluating the Long-Run Impacts of the 9/11 Terrorist Attacks on U.S. Domestic Airline Travel." *Applied Economics* 38, no. 4 (2006): 363–370.

Botha, Jan L., Marissa K. Neighbour, and Satnam Kaur. *An Approach for Actions to Prevent Suicides on Commuter and Metro Rail Systems in the United States* (MTI Report 12–33). San Jose, CA: Mineta Transportation Institute, 2014.

Bradbury, Steven G. *The Developing Legal Framework for Defensive and Offensive Cyber Operations*. Cambridge, MA: Harvard College, 2011.

Brandon, Susan E., and Andrew P. Silke. "Near and Long-Term Psychological Effects of Exposure to Terrorist Attacks." In *Psychology of Terrorism*, edited by Bruce Bongar, Lisa M. Brown, Larry E. Beutler, James N. Breckenridge, and Philip G. Zimbardo (175–193). New York: Oxford University Press, 2007.

Brezina, Corona. *Public Security in an Age of Terrorism*. New York: The Rosen Publishing Group, 2009.

Brito, Jerry, and Tate Watkins. "Loving the Cyber Bomb-the Dangers of Threat Inflation in Cybersecurity Policy." Working paper, Arlington, VA: Mercatus Center, George Mason University, 2011. http://mercatus.org/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy.

Bumiller, Elisabeth, and Thom Shanker. "Panetta Warns of Dire Threat of Cyberattack on US." *The New York Times*, October 11, 2012, sec. World.

Butler, Adrienne Stith, Allison M. Panzer, and Lewis R. Goldfrank, eds. *Preparing for the Psychological Consequences of Terrorism*. Washington, DC: National Academies Press, 2003. http://www.nap.edu/catalog/10717.html.

Butler, Lisa, Leslie Morland, and Gregory Leskin. "Psychological Resilience in the Face of Terrorism." In *Psychology of Terrorism*, edited by Bruce Bongar, Lisa M. Brown, Larry E. Beutler, James N. Breckenridge, and Philip G. Zimbardo (400–417). New York: Oxford University Press, 2007.

Cao, Liqun, Steven Stack, and Yi Sun. "Public Attitudes toward the Police: A Comparative Study between Japan and America." *Journal of Criminal Justice* 26, no. 4 (1998): 279–289.

Capra, Gregory S. "Protecting Critical Rail Infrastructure." *The Counterproliferation Papers, Future Warfare Series*, no. 38. Maxwell Air Force Base, AL: U.S. Air Force Counterproliferation Center, Air University, 2006.

Carafano, James Jay. "One Year Later: Lessons from Recovery after the Great Eastern Japan Earthquake." *Heritage Foundation Special Report*, no. 108, 2012. http://www.heritage.org/research/reports/2012/04/one-year-later-lessons-from-recovery-after-the-great-eastern-japan-earthquake.

Carafano, James Jay, Steve Bucci and Jessica Zuckerman. "Fifty Terror Plots Foiled since 9/11: The Homegrown Threat and the Long War on Terrorism." *Backgrounder 2682*, April 25, 2012. http://www.heritage.org/research/reports/2012/04/fifty-terror-plots-foiled-since-9-11-the-homegrown-threat-and-the-long-war-on-terrorism.

Central Japan Railway Company. *The Effect of Bomb Disposal at the Hamamatsu Workshop Site on Train Service*. Tokyo, Japan: Central Japan Railway Company, 2012.

———. *The Effect of Bomb Disposal at the Hamamatsu Workshop Site on Train Service*. Tokyo, Japan: Central Japan Railway Company, 2013.

Chaturvedi, Vaibhav, and Son H. Kim. “Long Term Energy and Emission Implications of a Global Shift to Electricity-Based Public Rail Transportation System.” *Energy Policy* 81 (2015): 176–185.

Chertoff, Michael. *FY 2006 Infrastructure Protection Program: Intercity Passenger Rail Security, Program Guidelines and Application Kit*. Washington, DC: U.S. Department of Homeland Security, Office of Grants and Training, 2005.

Colwill, Carl. “Human Factors in Information Security: The Insider Threat–Who can You Trust These Days?” *Information Security Technical Report* 14, no. 4 (2009): 186–196.

Cordner, Gary. “Community Policing: Elements and Effects (1995).” In *The Oxford Handbook of Police and Policing*, edited by Michael Dean Reisig, and Robert J. Kane (148–168). Oxford, UK: Oxford University Press, 2014.

Darken, Rudy, and Ted G. Lewis. “Potholes and Detours in the Road to Critical Infrastructure Protection Policy.” *Homeland Security Affairs* 1, no. 2 (2005): 1–11. https://www.hsaj.org/articles/177.

Davila, Vianna. “High-Speed Toll Road Opening.” *San Antonio Express-News*, October 24, 2012. Accessed November 26, 2014. http://www.mysanantonio.com/news/local_news/article/High-speed-toll-road-opening-3974705.php.

De Cillis, Francesca, Maria Carla De Maggio, Concetta Pragliola, and Roberto Setola. “Analysis of Criminal and Terrorist Related Episodes in Railway Infrastructure Scenarios.” *Journal of Homeland Security and Emergency Management* 10, no. 2 (2013): 447–476.

Dinning, Michael. “Introduction to Cyber Security Issues for Transportation.” Webinar, John A. Volpe National Transportation Systems Center. December 7, 2011. https://www.pcb.its.dot.gov/t3/s111207_cybersecurity.asp.

Dixon, Scott. “Texas to Get Shinkansen System.” *The Japan Times*, August 2, 2014. http://www.japantimes.co.jp/news/2014/08/02/business/economy-business/private-u-s-railway-wants-bullet-train-line-for-texas-by-2021/#.VB7cHhZ_TYQ.

Doll, Abby, Renee Pirrong, Matthew Jennings, George Stasny, Andy Giblin, Steph Shaffer, and Aimee Anderson. *Critical Infrastructure and Cyber Security*. College Station, TX: George Bush School of Government and Public Service, Texas A&M University, 2011.

DuBose, Michael. *The Insider Threat: Why Chinese Hacking May Be the Least of Corporate Worries*. New York: Kroll Advisory Solutions, 2013.

Erikkson, Jonas, and Anna-Karin Juhl. *Guide to Risk and Vulnerability Analyses*. Karlstad: Swedish Civil Contingencies Agency, 2012.

Federal Railroad Administration. *Dallas to Houston High-Speed Rail Environmental Impact Statement: Scoping Report*. Washington, DC: Federal Railroad Administration, 2015.

Fisher, Robert E., William Buehring, Ron Whitfield, Gib Bassett, David Dickinson, Rebecca Haffenden, Matilda Klett, Michelle Lawlor. *Constructing Vulnerability and Protective Measures Indices for the Enhanced Critical Infrastructure Protection Program* (no. ANL/DIS-09-4). Argonne, IL: Argonne National Laboratory, 2009. http://www.osti.gov/scitech/biblio/966343.

Fleming, Susan. "Positive Train Control: Additional Authorities could Benefit Implementation." U.S. General Accounting Office. Last modified September 16, 2013. Accessed November 15, 2015. http://www.gao.gov/products/GAO-13-720.

Freemark, Yonah. "Why Can't the United States Build a High-Speed Rail System?" The Atlantic's City Lab. August 13, 2014. http://www.citylab.com/politics/2014/08/why-cant-the-united-states-build-a-high-speed-rail-system/375980/.

Fujisaki, Ichiro. "Japan's Recovery Six Months after the Earthquake, Tsunami and Nuclear Crisis." Brookings Institution. Last modified September 9, 2011. Accessed June 21, 2015. http://www.brookings.edu/events/2011/09/09-japan-recovery.

Gaonjur, Pravesh, and Chandradeo Bokhoree. *Risk of Insider Threats in Information Technology Outsourcing: Can Deceptive Techniques be Applied?* Port Louis, Mauritius: University of Technology, 2006.

Glass, Tom. "Op-Ed: Texas must Protect our Grid against Attack—the Feds Won't." Breitbart Texas. Last modified April 19, 2015. Accessed November 15, 2015. http://www.breitbart.com/texas/2015/04/19/op-ed-texas-must-protect-our-grid-against-attack-the-feds-wont/.

Green, Stephen. "Company Planning High-Speed Rail Project." *The Huntsville Item*, October 1, 2014. http://www.itemonline.com/news/article_3c34e4b0-4907-11e4-b2dd-131f33bc7d85.html.

Greenberg, Michael, Paul J. Lioy, Burnur Ozbas, Nancy Mantell, Sastry Iskapalli, and Michael L. Lahr. "Passenger Rail Security, Planning, and Resilience: Application of Network, Plume, and Economic Simulation Models as Decision Support Tools." *Risk Analysis* 33, no. 11 (2013): 1969–1986.

Hayden, Michael V. "The Future of Things Cyber." *Strategic Studies Quarterly* (spring 2011): 1–5. http://www.au.af.mil/au/ssq/2011/spring/hayden.pdf.

Hughes, Christopher. "Japan's Security Policy, the US-Japan Alliance, and the 'War on Terror': Incrementalism Confirmed or Radical Leap?" *Australian Journal of International Affairs* 58, no. 4 (2004): 427–445.

Hobbing, Peter, and Rey Koslowski. *The Tools Called to Support the 'Delivery' of Freedom, Security and Justice: A Comparison of Border Security System in the EU and in the US*. Brussels: European Parliament, Directorate General for European Policies, 2009. http://www.europarl.europa.eu/RegData/etudes/note/join/2009/410681/IPOL-LIBE_NT%282009%29410681_EN.pdf.

Ito, Harumi, and Darin Lee. "Assessing the Impact of the September 11 Terrorist Attacks on U.S. Airline Demand." *Journal of Economics and Business* 57, no. 1 (2005): 75–95.

Jarmusz, T. S. "Disgruntled Employee Steals Train." *Gillette News Record*, October 12, 2014. Accessed November 23, 2014. http://www.gillettenewsrecord.com/news/local/article_53a59dd3-6d5c-5353-a3f4-3e1d53c83398.html.

Jenkins, Brian M. *Terrorism and the Security of Public Surface Transportation*. Santa Monica, CA: RAND Corporation, 2004.

Jenkins, Brian M., and Bruce R. Butterworth. "Mineta Transportation Institute Says Subways are Still in Terrorists' Sights." *PRN Newswire*, March 24, 2014. Accessed December 7, 2014. http://www.prnewswire.com/news-releases/mineta-transportation-institute-says-subways-are-still-in-terrorists-sights-252015231.html.

Jenkins, Brian M., Bruce R. Butterworth, and Jean-Francois Clair. *The 1995 Attempted Derailing of the French TGV (High-Speed Train) and a Quantitative Analysis of 181 Rail Sabotage Attempts*. San José, CA: Mineta Transportation Institute, 2010.

Jenkins, Brian M., Chris Kozub, Bruce R. Butterworth, Renee Haider, and Jean-Francois Clair. *Formulating a Strategy for Securing High-Speed Rail in the United States*. San José, CA: Mineta Transportation Institute, 2013.

Jenkins, Brian M., and Joseph Trella, *Carnage Interrupted: An Analysis of Fifteen Terrorist Plots against Public Surface Transportation*. San Jose, CA: Mineta Transportation Institute, 2012.

Johnsen, Michael. "Dallas to Houston High-Speed Rail—Passenger Service from Houston to Dallas." Federal Railroad Administration. Accessed September 21, 2014. https://www.fra.dot.gov/Page/P0700.

Jones, Morgan D. *The Thinker's Toolkit: Fourteen Powerful Techniques for Problem Solving*. New York: Three Rivers Press, 1998.

Kaiser, Kim. "High-Speed Rail Security Needs a Different Approach than Commuter Rail." *Mass Transit Magazine*, August 11, 2011. Accessed December 8, 2014. http://www.masstransitmag.com/article/10317151/high-speed-rail-security-needs-a-different-approach-than-commuter-rail.

Kerr, Paul K., John Rollins, and Catherine A. Theohary. *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*. Washington, DC: Congressional Research Service, 2010.

King, Rachel. "Anonymous Hacks BART Police website; Publishes Officers' Info." ZDNet. August 17, 2011. Accessed December 26, 2014. http://www.zdnet.com/article/anonymous-hacks-bart-police-website-publishes-officers-info/#!

Kissane, Dylan. "Terror on the TGV? The Terrorist Threat to France's High Speed Train Network." Paris: Centre d'Etudes Franco-Americain de Management, 2007.

LaFree, Gary, and Laura Dugan. "Introducing the Global Terrorism Database." *Terrorism and Political Violence* 19, no. 2 (2007): 181–204.

Landree, Eric, Christopher Paul, Beth Grill, Aruna Balakrishnan, and Bradley Wilson. *Freedom and Information: Assessing Publicly Available Data regarding U.S. Transportation Infrastructure Security*. Santa Monica, CA: Rand Corporation, 2007.

Laursen, Lucas. "Spanish High-Speed Train Crash Offers Safety-System Lessons." *Scientific American*, July 26, 2013. Accessed December 28, 2014. http://www.scientificamerican.com/article/ish-high-speed-train-crash/.

Lester B. Lave, Jay Apt, Alex Farrell, and M. Granger Morgan. "Increasing the Security and Reliability of the U.S. Electricity System." In *The Economic Impacts of Terrorist Attacks, Cheltenham, UK, and Northampton, Mass*, edited by Harry W. Richardson, Peter Gordon, James E. Moore, III, and Edgar Elgar (57–69). Cheltenham: Edward Elgar Publishing, Inc., 2005. https://ideas.repec.org/h/elg/eechap/3783_4.html.

Lerman, Amy E., and Vesla Weaver. "Staying Out of Sight? Concentrated Policing and Local Political Action." *The Annals of the American Academy of Political and Social Science* 651, no. 1 (2014): 202–219.

Litman, Todd. "Terrorism, Transit and Public Safety: Evaluating the Risks." *Journal of Public Transit* 8, no. 4 (2005): 33–46.

Maurillo, Donna R. "High-Speed Rail in the US: Will it be a More Attractive Terror Target than Inter-City Rail?" Master's thesis, San Jose State University, 2012.

McCaul, Michael T. and Peter King. *Majority Staff Report on the National Network of Fusion Centers*. United States House of Representatives Committee on Homeland Security. Accessed November 24, 2014. https://homeland.house.gov/files/documents/CHS%20SLFC%20Report%202013%20FINAL.pdf.

McCoy, Luke. “Did You Know That Your Texas Concealed Handgun License is Now a Valid Proof of Identification?” USA Carry. September 23, 2015. http://www.usacarry.com/texas-concealed-handgun-license-valid-id/.

Meyer, Sunniva F. “Preventing Mass Killings: Determining the Optimal Allocation of Security Resources between Crowded Targets.” *Peace Economics, Peace Science and Public Policy* 17, no. 1 (2011).

Morag, Nadav. *Comparative Homeland Security: Global Lessons*. Wiley Series on Homeland Defense and Security. Hoboken, NJ: John Wiley and Sons, 2012. Kindle edition.

Morgan, M. Granger. *Terrorism and the Electric Power Delivery System*. Washington, DC: National Academies Press, 2012.

Morimura, Tsutomu. *Introduction of the N700-I Bullet*. Nagoya, Japan: Central Japan Railway Company, 2010.

Moore, Michael Scott. “High-Speed Rail’s Weak Link is Security.” *Pacific Standard*, May 4, 2011. Accessed October 27, 2014. http://www.psmag.com/navigation/politics-and-law/high-speed-rails-weak-link-is-security-30874/.

Mott, Amanda. “Should the Threat of a Terrorist Attack on a Nuclear Power Plant be Considered under NEPA Review.” *UCLA Journal of International Law and Foreign Affairs* 12 (2007): 333–358.

Mulrine, Anna. “Cyber Security: The New Arms Race for a New Front Line.” *Christian Science Monitor*, September 15, 2013. Accessed December 27, 2014. http://www.csmonitor.com/USA/Military/2013/0915/Cyber-security-The-new-arms-race-for-a-new-front-line.

Murray-Tuite, Pamela M., and Xiang Fei. “A Methodology for Assessing Transportation Network Terrorism Risk with Attacker and Defender Interactions.” *Computer-Aided Civil and Infrastructure Engineering* 25, no. 6 (2010): 396–410.

Myers, David G. “Do We Fear the Right Things.” *APS Observer* 14, no. 3 (2001): 31. Accessed December 6, 2015. http://www.psychologicalscience.org/index.php/publications/observer/2001/december-01/do-we-fear-the-right-things.html.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. Washington, DC: Government Printing Office, 2011.

National Institute of Standards and Technology. *Cybersecurity Framework Development Overview*. Washington, DC: National Institute of Standards and Technology, 2013.

Nishiyama, Takao. *High-Speed Rail Operations in Japan*. New York: Japan Railways Group, 2010.

Nobuo Mimura, Kazuya Yasuhara, Seiki Kawagoe, Hiromune Yokoki, and So Kazama. "Damage from the Great East Japan Earthquake and Tsunami: A Quick Report." *Mitigation and Adaptation Strategies for Global Change* 16, no. 7 (2011): 803–818. 7.

Patil, Sunil Bhanu Patruni, Hui Lu, Fay Dunkerley, James Fox, Dimitris Potoglou, and Neil Robinson. "Privacy Vs Security?" *RAND Europe Research Brief* (2015). http://www.rand.org/pubs/research_briefs/RB9843z1.html.

Paulson, Bob. "RCMP Arrests Two Individuals for Terrorism-Related Charges." Royal Canadian Mounted Police. April 22, 2013. Accessed November 23, 2014. http://www.rcmp-grc.gc.ca/news-nouvelles/2013/04-22-ns-sn-eng.htm.

Perry, Rick. *Texas Homeland Security Strategic Plan: 2010–2015*. Austin, TX: Texas Department of Public Safety, 2010.

Peplow, Douglas E., C. David Sulfredge, Robert L. Sanders, Robert H. Morris, and Todd A. Hann. "Calculating Nuclear Power Plant Vulnerability using Integrated Geometry and Event/Fault-Tree Models." *Nuclear Science and Engineering* 146, no. 1 (2004): 71–86.

Peterman, David R. *Passenger Rail Security: Overview of Issues*. Washington, DC: Congressional Research Service, 2005.

Powner, David. *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity*. Washington, DC: U.S. Government Accountability Office, 2005. http://www.gao.gov/assets/120/111987.pdf.

Reaves, Brian A. "Census of State and Local Law Enforcement Agencies, 2008." last modified July 2011. Accessed June 22, 2015. http://www.bjs.gov/index.cfm?ty=pbdetail&iid=2216.

Reddy, M. Kameswara, K. V. S. Srinadh, T. V. Ravi Teja, and Rafiuzzama Shaik. "Stress Analysis on Behaviour of Rails." *International Journal of Engineering Research* 4, no. 1 (2015): 4–8. http://works.bepress.com/cgi/viewcontent.cgi?article=1431&context=irpindia.

Rice, Mason, Robert Miller, and Sujeet Shenoi. "May the U.S. Government Monitor Private Critical Infrastructure Assets to Combat Foreign Cyberspace Threats?" *International Journal of Critical Infrastructure Protection* 4, no. 1 (2011): 3–13.

Richards, Anne L. *DHS Grants Used for Mitigating Risks to Amtrak Rail Stations*. Washington, DC: Department of Homeland Security, Office of Inspector General, 2011.

Rollins, John, and Anna Henning. *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*. Washington, DC: Congressional Research Service, 2009.

Rosenzweig, Paul. *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World*. Santa Barbara, CA: Praeger, 2013.

Rudner, Martin. "Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge." *International Journal of Intelligence and Counter Intelligence* 26, no. 3 (2013): 453–481.

Ryal, Julian**.** "Bullet Train at 50: Rise and Fall of the World's Fastest Train." *The Telegraph*. Last modified October 1, 2014. Accessed June 21, 2015. http://www.telegraph.co.uk/news/worldnews/asia/japan/11133241/Bullet-train-at-50-rise-and-fall-of-the-worlds-fastest-train.html.

Sabzehparvar, Majid, and Seyyed Hossein Alavi. "The Role of Key Parameters in Public Transportation Security." *Journal of Transportation Security* 8, no. 1–2 (2015): 37–40.

Sakelaris, Nicholas. "High-Speed Rail Station Will be 'Iconic' Part of Dallas Skyline, CEO Says." *Dallas Business Journal*, November 21, 2014.

Scieszinski, Robert. "Positive Train Control (PTC) Overview (Railroad Safety)." Federal Railroad Administration. Accessed November 23, 2014. http://www.fra.dot.gov/Page/P0621.

Scovel, Calvin. *DOT Has Made Progress but Significant Weaknesses in its Information Security Remain*. Washington, DC: U.S. Department of Transportation, 2014.

Serrano, Jody. "High-Speed Rail Firm's Chief: Public Meetings Set for Proposal." *The Texas Tribune,* September 20, 2014.

Slavo, Mac. "Feds Threaten Texas with No-fly Zone over Anti-TSA Legislation." SHTFPlan. May 25, 2011, http://www.shtfplan.com/headline-news/feds-threaten-texas-with-no-fly-zone-over-anti-tsa-legislation_05252011.

Sneider, Julie. "Railroad Communication and Signal Article - Railroads Gear Up to Protect Computers from Hackers." *Progressive Railroading Magazine,* September 2012. Accessed November 23, 2014. http://www.progressiverailroading.com/c_s/article/Railroads-gear-up-to-protect-computers-from-hackers--32354.

Strandberg, Veronica. "Rail Bound Traffic: A Prime Target for Contemporary Terrorist Attacks?" *Journal of Transportation Security* 6, no. 3 (2013): 271–286.

\

Stephenson, Will. “The Story of Jason Woodring, the Arkansas Power Grid Vandal.” *Arkansas Times*, June 12, 2014. Accessed December 28, 2014. http://www.arktimes.com/arkansas/the-story-of-jason-woodring-the-arkansas-power-grid-vandal/Content?oid=3334926.

Sternstein, Aliya. “Hackers Manipulated Railway Computers, TSA Memo Says.” *Government Executive*, January 23, 2012. http://www.nextgov.com/cybersecurity/2012/01/hackers-manipulated-railway-computers-tsa-memo-says/50498.

Stewart, Mark G., Michael Netherton, Yuhua Shi, Matthew Grant, and John Mueller. “Probabilistic Terrorism Risk Assessment and Risk Acceptability for Infrastructure Protection.” *Australian Journal of Structural Engineering* 13, no. 1 (2012): 1–18.

Straub, Detmar W. “The Effect of Culture on IT Diffusion: Email and FAX in Japan and the US.” *Information Systems Research* 5, no. 1 (1994): 23–47.

Talianova, Julia. “Cantor Fitzgerald, American Airlines Settle 9/11 Lawsuit.” *CNN*, December 17, 2013. http://www.cnn.com/2013/12/17/us/new-york-cantor-fitzgerald-american-settlement/index.html.

Tamura, Akihiko. *An Overview of Japan’s High Speed Rail: Shinkansen*. Tokyo, Japan: Ministry of Land, Infrastructure, Transport, and Tourism, 2012.

Taylor, Brian D. “Terrorist Attacks and Transport Systems.” *ACCESS Magazine* 1, no. 28 (2006).

Taylor, Anthony J. W. “Defusing the Terrorism of Terror.” In *Psychology of Terrorism*, edited by Bruce Bongar, Lisa M. Brown, Larry E. Beutler, James N. Breckenridge, and Philip G. Zimbardo (373–399). New York: Oxford University Press, 2007. Kindle edition.

Testar, Jason. “What Tokyo Taught Us.” *Homeland Defense Journal* 1, no 3 (June: 2003): 34–39.

Texas Legislative Council. *Texas Government Code, Chapter 421: Homeland Security*. Austin, TX: Texas Legislative Council, 2003.

Turk, Robert J. *Cyber Incidents Involving Control Systems*. Idaho Falls, ID: Idaho National Engineering and Environmental Laboratory, 2005.

Unisys Corporation. *Critical Infrastructure: Security Preparedness and Maturity*. Blue Bell, PA: Unisys Corporation, 2014.

U.S. Census Bureau. “2010 Census Urban and Rural Classification and Urban Area Criteria.” last modified February 9, 2015. http://www.census.gov/geo/reference/ua/urban-rural-2010.html.

U.S. Department of Homeland Security. *Sector Risk Snapshots*. Washington, DC: U.S. Department of Homeland Security, Office of Cyber and Infrastructure Analysis, 2014. http://nacchopreparedness.org/wp-content/uploads/2014/05/OCIA-Sector-Risk-Snapshots.pdf.

Vale, Madeline. *Securing the U.S. Electrical Grid*. Washington, DC: Center for the Study of the Presidency and Congress, 2014.

Vock, Daniel C. “Feds Push Gently on ‘REAL ID,’” Pew Trusts. January 22, 2014. http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2014/01/22/feds-push-gently-on-real-id.

Vohra, Pulkit. “Cyber Security: Insider Threats—Government’s Role in Protecting India’s Critical Infrastructure Sectors.” Master’s thesis, University of Warwick, 2014.

Weiser, Benjamin. “Last 9/11 Wrongful-Death Suit is Settled.” *The New York Times*, September 19, 2011.

Wheeler, John, and John D. L. Wheeler. *An Independent Review of Airport Security and Policing for the Government of Australia*. Canberra: Department of Transport and Regional Services, 2005.

White House. *The Comprehensive National Cybersecurity Initiative*. Washington, DC: The White House, 2010.

Wijesekera, Duminda. “Critical Rail Infrastructure Protection Research at George Mason University.” *The Critical Infrastructure Report* 7, no. 8 (2009).

Wilshusen, Gregory. *Critical Infrastructure Protection: Cybersecurity Guidance is Available, but More Can Be Done to Promote Its Use*. Washington, DC: Government Accountability Office, 2011. http://www.gao.gov/products/GAO-12-92.

Wilson, Jeremy M. *Securing America’s Passenger-Rail Systems*. Santa Monica, CA: Rand Corporation, 2007.

Wolf, Naomi. *The End of America: Letter of Warning to a Young Patriot*. White River Junction, VT: Chelsea Green Publishing, 2007.

Wray, Dianna, and Eric Nicholson. “What Will a Bullet Train Mean for the Future of Texas?” *Houston Press*. Last modified August 18, 2015. Accessed October 8, 2015. http://www.houstonpress.com/news/on-the-line-will-the-houston-dallas-bullet-train-revolutionize-texas-or-divide-it-forever-7679365.

Yates, Justin, Rajan Batta, and Mark Karwan. “Optimal Placement of Sensors and Interception Resource Assessment for the Protection of Regional Infrastructure from Covert Attack.” *Journal of Transportation Security* 4, no. 2 (2011): 145–169.

Zetter, Kim. “A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever.” *Wired*. Last modified January 8, 2015. Accessed November 14, 2015. http://www.wired.com/2015/01/german-steel-mill-hack-destruction/.

# INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California